

USTIP

User Manual

Raritan Computer Inc.

400 Cottontail Lane
Somerset, NJ 08873
USA
Tel. 1-732-764-8886
Fax. 1-732-764-8887
E-mail: sales@raritan.com
<http://www.raritan.com/>

Raritan Computer Japan, Inc.

4th Flr. Shinkawa NS Building
1-26-2 Shin-kawa, Chuo-ku
Tokyo 104-0033
Japan
Tel. 81-03-3523-5991
Fax. 81-03-3523-5992
E-mail: sales@raritan.co.jp
<http://www.raritan.co.jp>

Raritan Computer France

120 Rue Jean Jaures
93200 Levallois-Perret
France
Tel. 33-14-756-2039
Fax. 33-14-756-2061
E-mail: sales.france@raritan.com
<http://www.raritan.fr>

Raritan Computer U.K. Ltd.

36 Great St. Helen's
London
EC3A 6AP
United Kingdom
Tel. 44 20 7614 7700
Fax. 44 20 7614 7701
E-mail: sales.uk@raritan.com
<http://www.raritan.com>

Raritan Computer Europe, B.V.

Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel. 31-10-284-4040
Fax. 31-10-284-4049
E-mail: sales.europe@raritan.com
<http://www.raritan.com/>

Raritan Computer Taiwan, Inc.

5F, 121, Lane 235,
Pao-Chiao Rd., Hsin Tien
Taipei Hsien
Taiwan, ROC
Tel. 886-2-8919-1333
Fax. 886-2-8919-1338
E-mail: sales.asia@raritan.com
<http://www.raritan.com.tw>

Raritan Computer Deutschland GmbH

Lichstraße 2
D-45127 Essen
Germany
Tel. 49-201-747-9820
Fax. 49-201-747-9850
E-mail: sales.germany@raritan.com
<http://www.raritan.de>

Shanghai Representative Office of Raritan Computer, Inc.

RM 17E Cross Region Plaza
899 Lingling Road
Shanghai China 2000030
Tel. 86-21-5425-2499
Fax. 86-21-5425-3992
E-mail: sales.china@raritan.com
<http://www.raritan.com.cn/>



Copyright ©2005 Raritan Computer, Inc.

USTIP-OC-E

June 2005

255-31-0006

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

Trademark Information

Product names mentioned in this document are trademarks or registered trademarks of their respective companies. UST-IP, Paragon, MasterConsole MX⁴, MasterConsole II, MasterConsole, and their respective logos are trademarks or registered trademarks of Raritan Computer, Inc. PS/2, RS/6000, and PC/AT are registered trademarks of International Business Machines Corporation. Sun is a registered trademark of Sun Microsystems. Microsoft and Windows are registered trademarks of Microsoft Corporation. All other marks are the property of their respective owners.

Japanese Approvals

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

For assistance in the U.S., please contact the Raritan Technical Support Team by telephone (732) 764-8886, by fax (732) 764-8887, or e-mail us at tech@raritan.com. Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm, EST.

For assistance outside the U.S., please contact your regional Raritan office.

Login

- The default UST-IP login user name is **admin**, and the default password is **raritan**. This user has administrative privileges.
- Passwords are case sensitive and must be entered in the exact case combination in which they were created.
- The default password **raritan** must be entered entirely in lowercase letters.
- To ensure security, change the default password as soon as possible.

Default IP Address

- UST-IP ships with the default IP address of 192.168.0.192

Firmware

- This manual applies to UST-IP Firmware v4.1 and above.

Contents

Chapter 1: Introduction	1
Overview	1
Access via Internet, LAN/WAN, or dial-up Modem.....	1
Product Photos.....	1
Product Features.....	1
Terminology	2
Chapter 2: Installation.....	3
Configuring Target Servers.....	3
Server Video Resolution.....	3
Windows XP Settings	3
Windows 2000 / ME Settings.....	3
Windows 95 / 98 / NT Settings	3
Linux Settings	4
Sun Solaris Settings	4
Apple Macintosh Settings	4
Apple Macintosh Settings.....	5
Configuring Network Firewall Settings.....	5
Physical Connections	5
USTIP Local Admin Console Port	5
Network Port.....	5
External Modem	5
Initial Configuration	6
Connect to UST-IP Remotely.....	8
Launch Raritan Remote Client (RRC).....	8
Establish a Connection.....	9
Note to CommandCenter Users.....	9
Chapter 3: Raritan Remote Client	11
Invoking Raritan Remote Client (RRC) via Web Browser.....	11
Security Settings.....	11
Launching Raritan Remote Client	11
Removing RRC from Browser Cache.....	12
Optional: Installing Raritan Remote Client Software.....	13
RRC Window Layout.....	13
RRC Navigator	14
Navigator Options.....	15
Creating New Profiles.....	15
Establishing a New Connection.....	17
Closing a Remote Connection.....	17
RRC Toolbar and Shortcuts.....	18
RRC Status Bar.....	19
Remote KVM Console Control.....	20
Single Mouse Mode / Dual Mouse Mode	21
Full Screen Mode	21
Keyboard Macros	22
Connection and Video Properties.....	25
Color Calibration.....	28
Remote Device Administration.....	29
Configuration Menus	29
Firmware Upgrade.....	29
Device Restart	29
Device Configuration Backup and Restore	29
Log Files	29
Chapter 4: Administrative Functions	31
Accessing the Administrative Functions	31
Local Admin Console.....	31
Remote Admin Console.....	32
Navigating the Administrative Menus.....	32
Network Configuration.....	33
User Station Options	34
Security Configuration.....	34
Performance Settings.....	36

Time and Date.....	37
Access Control List	38
Remote Syslog.....	39
View UST-IP Status	40
Restart or Shutdown the UST-IP	40
Diagnostics.....	41
Appendix A: Specifications	43
Remote Connection	43
Raritan Remote Client (RRC) Software	43
KVM Input	43
Cable Specifications.....	43
KVM Switch Specifications	43
Output Specifications	43
Appendix B: SNMP Features.....	45
Appendix C: Frequently Asked Questions.....	47
Appendix D: Troubleshooting	51
Problems and Suggested Solutions.....	51
Event Log File and On-Screen Error Codes	56

Chapter 1: Introduction

Overview

Congratulations on your purchase of UST-IP, the industry-leading solution for multi-platform, high-performance, network-based, remote KVM console access. UST-IP enables highly-secure, multi-user, bandwidth-efficient, and software-independent access to your servers' KVM consoles via a web browser.

UST-IP uses Raritan's powerful frame-grabber and Video Compression Algorithm to capture, digitize, and compress the video signal before transmitting to a remote PC. The remote user has direct access and total control of target servers for maintenance, administration, and trouble-shooting, from running GUI applications to BIOS-level troubleshooting, and even rebooting.

Use UST-IP for convenient access to servers anytime, from anywhere:

- Control servers from within the building or across a campus
- Manage servers at branch offices from a central site
- Provide remote support for worldwide data centers
- Troubleshoot, reconfigure, and reboot servers from home
- Provide convenient and secure lights-out server management

Access via Internet, LAN/WAN, or dial-up Modem

UST-IP provides a broad array of remote access methods to control any server connected to a Raritan KVM Switch. Since servers can also be accessed out-of-band with UST-IP, remote access to mission-critical target servers is always available - even if the network is down.

Product Photos



Product Features

Access

- Remote KVM access via the Internet, LAN/WAN, or dial-up modem
- Up to two simultaneous user throughput to switch(es) or server(s)
- Up to 16 simultaneous users (using PC-share mode)
- Web browser accessible
- Remote access to serial devices (VT100) connected to UST-IP serial port

Performance

- Superior compression algorithm for exceptional performance
- No impact on target server performance
- Automatic sensing of video resolution for optimum display
- High-performance mouse tracking and synchronization

Reliability

- External modem using a dedicated modem port allows servers to be accessible even if network is unavailable

Security

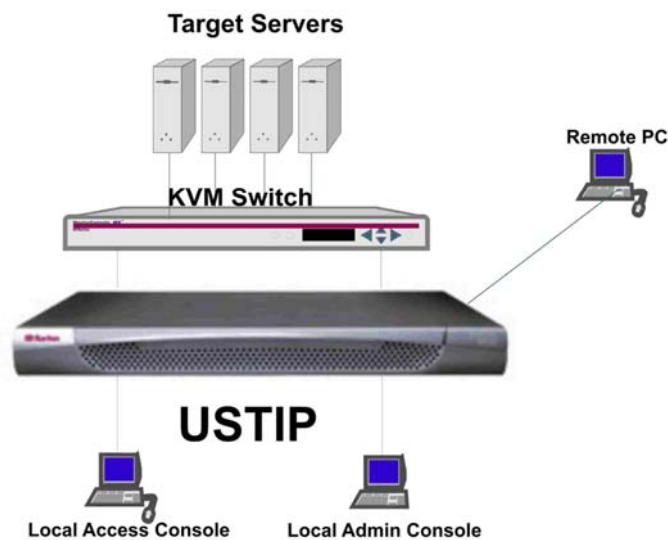
- SSL 128-bit RSA public key, 128-bit RC4 private key encryption
- Single, configurable TCP port for firewall protection

Administration

- Remote Administration via Web Browser interface
- SNMP Support
- Simplified installation and user interface
- User console for direct analog access to KVM switch
- Extensive downloadable user event log
- DHCP or fixed IP addressing

Terminology

This manual makes use of the following terms to indicate components of a typical UST-IP configuration. While reading the manual, please refer to the diagram below for clarification when necessary.



Target Server(s)	Servers to be accessed remotely via UST-IP and its connected KVM configuration.
Remote PC	A Windows-based computer used to access and control target servers connected to UST-IP.
Local Access Console	A user console consisting of a PS/2 keyboard, PS/2 mouse, and VGA monitor, directly attached to UST-IP to control target servers locally (not through the network). Single-port UST-IP models (UST-IP1) allow connection of one local access console.
Local Admin Console	A VT100 terminal directly attached to UST-IP, used for administration and setup. From this console, you can access UST-IP administration menus directly. You cannot view Target Servers of the connected KVM configuration using this screen. Although UST-IP also allows remote administration via the network, the local admin console provides the most convenient means to perform initial setup.

Chapter 2: Installation

Configuring Target Servers

Before installing UST-IP, first configure any target servers that you wish to access via UST-IP, in order to ensure optimum performance, as outlined below. Note that the following configuration requirements apply only to *target servers*, not to the computers that you will be using to access UST-IP remotely.

Server Video Resolution

For optimal bandwidth efficiency and video performance, target servers running graphical user interfaces such as Windows, X-Windows, Solaris, and KDE should be configured with desktop backgrounds set to a predominantly solid, light-colored graphic. Backgrounds featuring photos or complex gradients should be avoided.

Ensure that the server's video resolution and refresh rate are supported by UST-IP, and that the signal is non-interlaced. UST-IP supports the following video resolutions:

Text Modes

640x480 @ 60Hz	1024x768 @ 60Hz
640x480 @ 72Hz	1024x768 @ 70Hz
640x480 @ 75Hz	1024x768 @ 75Hz
640x480 @ 85Hz	1024x768 @ 85Hz
800x600 @ 56Hz	1152x864 @ 60Hz
800x600 @ 60Hz	1152x864 @ 75Hz
800x600 @ 72Hz	1280x1024 @ 60Hz
800x600 @ 75Hz	
800x600 @ 85Hz	

Windows XP Settings

On target servers running Microsoft Windows XP, disable the “Enhanced Pointer Precision” option, and set the mouse motion speed exactly to the middle speed setting. These parameters are found in: **Start → Settings → Control Panel → Printers and Other Hardware → Mouse → Pointer Options.**

Note: For Target Servers running Windows NT, 2000, or XP, you may wish to create a username to be used only for remote connections through UST-IP. This allows you to keep the Target Server's slow mouse pointer motion/acceleration settings exclusive to the UST-IP connection only, as other users may desire faster mouse speeds.

Note: Windows XP and 2000 login screens revert to pre-set mouse parameters that differ from those suggested for optimal UST-IP performance; therefore, mouse sync will not be optimal at these screens. If you are comfortable adjusting the registry on Windows target servers, you can obtain better UST-IP mouse synchronization at login screens by using the Windows registry editor to change the following settings: Default user mouse motion speed = 0; mouse threshold 1 = 0; mouse threshold 2 = 0.

Windows 2000 / ME Settings

On target servers running Microsoft Windows 2000 / ME, set the mouse pointer acceleration to “none” and the mouse motion speed exactly to the middle speed setting. These parameters are found in: **Start → Settings → Control Panel → Mouse → Motion.**

Windows 95 / 98 / NT Settings

On target servers running Microsoft Windows 95 / 98 / NT, set the mouse motion speed to the slowest setting in **Start → Settings → Control Panel → Mouse → Motion.**

Linux Settings

On target servers running Linux graphical interfaces, set the mouse acceleration to exactly 1 and set threshold to exactly 1.

As mentioned above, please ensure that each target server running Linux is using a resolution supported by UST-IP at a standard VESA resolution and refresh rate. Each Linux target server should also be set so the blanking times are within +/- 40% of VESA standard values.

To check for these parameters:

- Go to the Xfree86 Configuration file XF86Config
- Using a text editor, disable all non-UST-IP supported resolutions
- Disable the virtual desktop feature, which is not supported by UST-IP
- Check blanking times (+/- 40% of VESA standard).
- Restart computer

Note: In many Linux graphical environments, the command <Ctrl+Alt+Plus> will change the video resolution, scrolling through all available resolutions that remain enabled in the XF86Config file.

Sun Solaris Settings

All target servers must be configured to one of the display resolutions supported by UST-IP. The most popular supported resolutions for Sun machines are:

- 1024x768@60Hz
- 1024x768@70Hz
- 1024x768@75Hz
- 1024x768@85Hz
- 1152x900@66Hz
- 1152x900@76Hz
- 1280x1024@60Hz

Target servers running the Solaris operating system must output VGA video (H-and-V sync, not composite sync). To change your Sun video card output from composite sync to the non-default VGA output, first issue the **Stop+A** command to drop to bootprom mode. Then, issue the command:

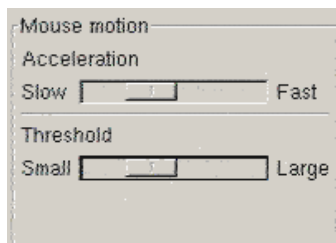
```
setenv output-device screen:r1024x768x70
```

to change the output resolution. Issue the “boot” command to reboot the server.

Alternatively, you may contact your Raritan representative to purchase a video output adapter. 13W3 Suns with composite sync output require APSSUN II Raritan guardian for use with UST-IP. HD15 Suns with composite sync output require 1396C Raritan converter to convert from HD15 to 13W3 and an APSSUN II Raritan guardian converter to support composite sync. HD15 Suns with separate sync output require an APKMSUN Raritan guardian for use with UST-IP.

Note that KVM switch brands other than Raritan’s may or may not properly handle PS/2-to-Sun signals.

On target servers running the Solaris operating system, set the mouse acceleration value to exactly 1 and threshold to exactly 1. Set this at the graphical user interface (shown below), or with the command line “xset mouse a t” where “a” is the acceleration and “t” is the threshold.



Apple Macintosh Settings

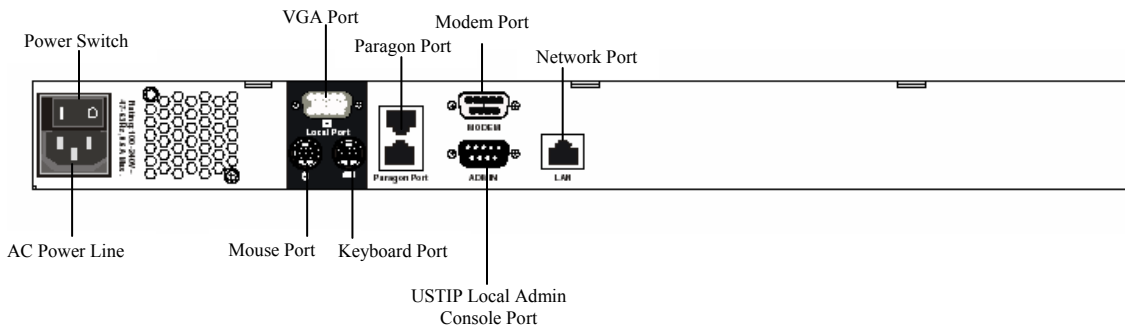
For target servers running an Apple Macintosh operating system, while using UST-IP to access and control your target server, you must set the UST-IP client (Raritan Remote Client) to “single cursor” mode. Dual cursor mode is not supported, and the two mouse pointers will not appear in sync if you attempt to control a Macintosh server via UST-IP in dual cursor mode.

Configuring Network Firewall Settings

If you wish to access UST-IP through a network firewall, your firewall must allow communication on TCP Port 5000. Alternatively, UST-IP can be configured to use a different TCP port of your own designation (see **Chapter 4: Administrative Functions, Network Configuration**).

In order to take advantage of UST-IP's web-access capabilities, the firewall must allow inbound communication on TCP Port 443 – the standard TCP port for HTTPS communication. In order to take advantage of UST-IP's redirection of HTTP requests to HTTPS (so that users may type the more common, "http://192.168.0.192", instead of "https://192.168.0.192"), then the firewall must allow inbound communication on TCP Port 80 – the standard TCP port for HTTP communication.

Physical Connections



USTIP Local Admin Console Port

Attach a VT100 terminal to the indicated ports (see diagram above) in the back of UST-IP.

Network Port

Connect a standard Ethernet cable from the network port to an Ethernet switch, hub, or router.

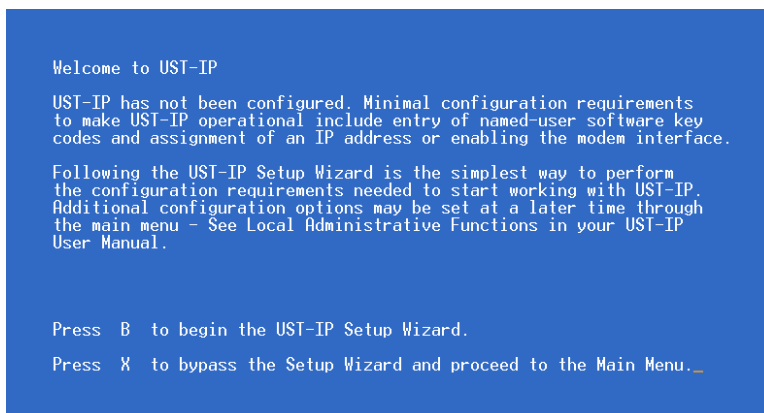
External Modem

For UST-IP, an external serial modem must be connected to the serial modem port.

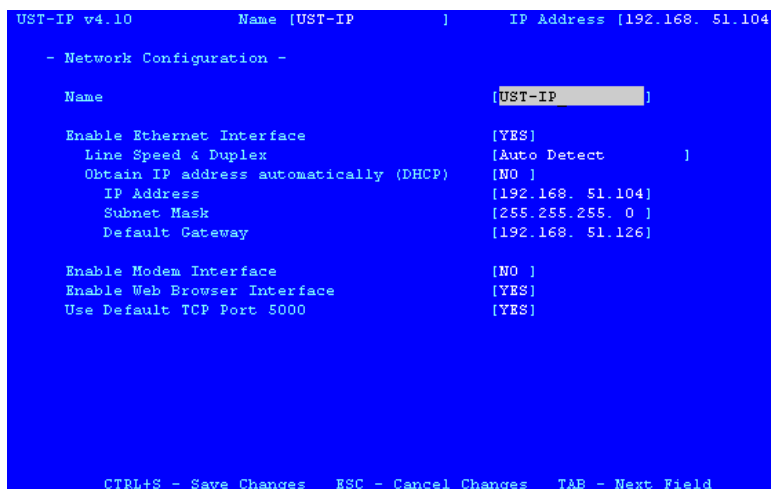
Initial Configuration

During initial configuration, the **UST-IP Setup Wizard** helps you quickly set up UST-IP for the first time. The UST-IP Setup Wizard appears only when accessing the Administrative Menus on an unconfigured UST-IP, and guides you through initial configuration parameters. The easiest way to perform this initial configuration is by using the Local Admin Console (see ‘Physical Connection’ instructions in the previous sections).

1. Power ON UST-IP via the power switch on the back of the UST-IP unit.
2. The Welcome to UST-IP Setup Wizard Screen will appear on the Local Admin Console.



3. Press the letter on the Local Admin Console keyboard to begin the UST-IP Setup Wizard.
4. The Network Configuration Screen appears.



5. Use the <Tab>, <↑> or <↓> keys to select each line on the Network Configuration screen and the <space bar>, or the <←> or <→> keys to toggle between available entries. Press the <Enter>, <Tab> or <↓> keys when your entry on each line is complete. Below are descriptions of each field, and the appropriate values to assign.
 - **Name:** Designate a unique name for this UST-IP unit, for example, “MiamiDataCenter.” (NOTE: no spaces; alphanumeric characters allowed?) The default name is **UST-IP**.
 - **Enable Ethernet Interface:** Designates whether UST-IP should enable its Ethernet adapter as active (default: YES).

Note: Network connections must be 10BASE-T or 100BASE-TX Ethernet

- **Line Speed & Duplex:** Enter the visual efficiency for the monitor: Auto detect 10 Mbps/Full Duplex, 10 Mbps/Half Duplex, 100 Mbps/Full Duplex, or 100 Mbps/Half Duplex
- **Obtain IP address automatically (DHCP):**

- ◆ **YES:** Enables dynamic IP addressing for UST-IP. Each time UST-IP boots, it requests an IP address from the local DHCP server. Note that this setting can make remote access to UST-IP from outside the LAN difficult, since the dynamically assigned IP address must be known in order to initiate a connection.
- ◆ **NO (default):** Assigns a fixed IP address to the UST-IP unit (recommended).
 - **IP Address:** Enter the IP address for UST-IP given by your Network Administrator.
 - **Subnet Mask:** Enter a Subnet Mask provided by your Network Administrator.
 - **Default Gateway:** Enter the Default Gateway if your Network Administrator specifies one.
- **Enable Modem Interface:** Enables Dial-up Modem access (default: YES). For UST-IP, an external serial modem must be connected in order for this function to work properly.
- **Enable Web Browser Interface:** Enables Web browser access to UST-IP (default: YES).
- **Use Default TCP Port 5000:**
 - **YES (default):** Utilizes the default port 5000.
 - **NO:** Enter an alternate port number.

Note: In order to access UST-IP from beyond a firewall, your firewall settings must enable two-way communication through the default port 5000 or the non-default port configured above.

6. Press **Ctrl+S** to save entries. The Main Menu will appear.
7. On the Main Menu, select **[R] Restart or shutdown the UST-IP**, and press the **Enter** key.
8. When prompted, press the letter **R** on your keyboard to restart UST-IP.
9. UST-IP will restart and the UST-IP Initialization screen appears upon boot up.
10. Congratulations! UST-IP is now ready for initial connection.

Accessing UST-IP Local Admin Port

To access the local admin console port from your UST-IP device, use HyperTerminal to configure specific settings for a PC and at least one additional setting for a laptop computer. Please perform the following steps:

- a. In Windows, click on the Start menu. Click Programs, then click Accessories, click Communications, and then click HyperTerminal to start a session.
- b. Name the session, select a session icon if required, and click OK.
- c. In the Connect To window, click on the Connect Using drop-down arrow and select COM1 (or other option, depending on where your PC's serial cable is connected).
- d. Click OK.
- e. In the COM1 Properties window, click on the Port Settings tab:
 - i. Click on the Bits per second drop-down arrow and select 115200.
 - ii. Click on the Flow control drop-down arrow and select NONE.
 - iii. Click OK.
- f. On the File menu, click Properties, and then click on the Settings tab:
 - i. Click on the Emulation drop-down arrow and select VT100.
 - ii. Click ASCII Setup. In the ASCII Setup window, ensure that only the option Wrap lines that exceed terminal width is checked. If any other options are checked, you may have display issues.
 - iii. Click OK.
 - iv. Click Terminal Setup. In the Terminal Settings window, ensure the option Keypad application mode is checked (this option must be specified for most laptop computers).
- g. Click OK.
- h. Click OK.

Proceed to the next section to initiate your first remote connection to UST-IP. After you have become familiar with the remote operation of UST-IP, consult **Chapter 4: Administrative Functions** to review the complete administrative functions provided by UST-IP.

Connect to UST-IP Remotely

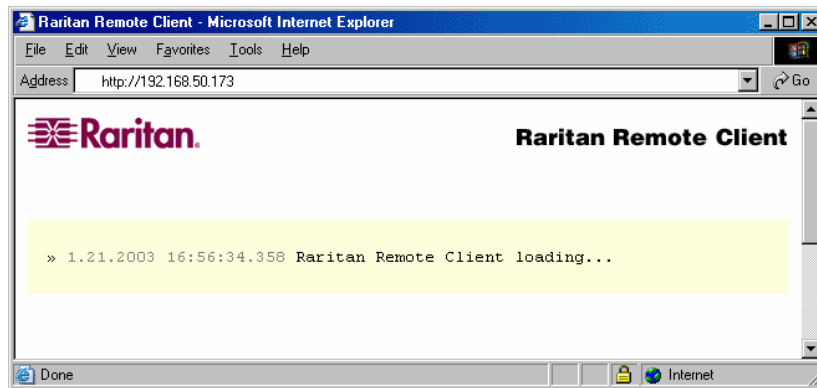
Having completed the physical installation of UST-IP, you are now ready to establish an initial network connection. Below are basic instructions for doing so. Please see **Chapter 3: Raritan Remote Client** for detailed instructions, being sure to review the “Remote KVM Console Control” and “Color Calibration” sections to optimize your UST-IP performance.

Launch Raritan Remote Client (RRC)

1. Log into any Windows-based computer with network access to UST-IP.
2. If you are using Windows NT, 2000, or XP, ensure that you are not a “restricted” user.
3. Launch Microsoft Internet Explorer. Ensure that your Internet Explorer security settings allow the download and execution of ActiveX controls.

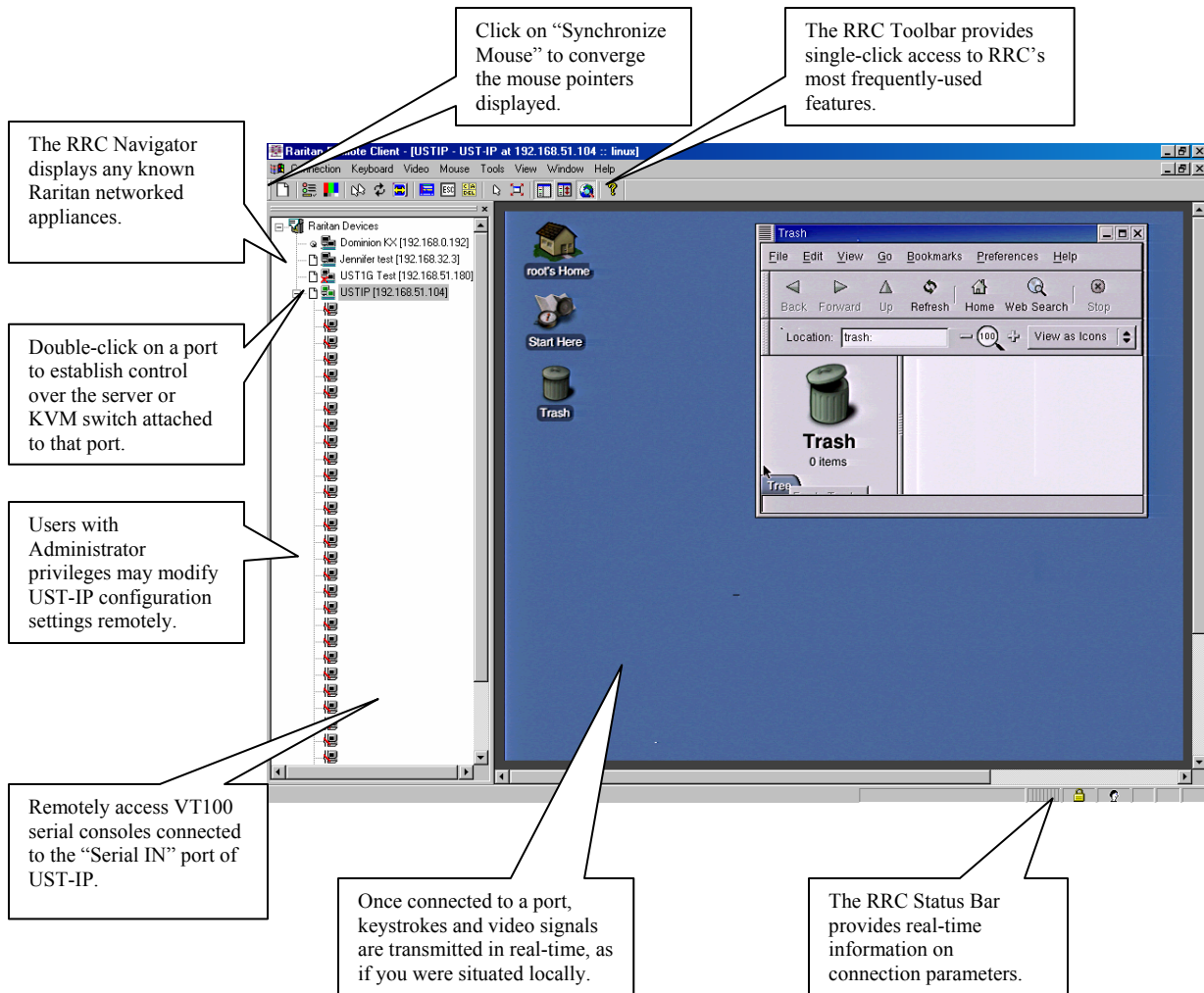
Note: The Windows default security setting of “Medium” is sufficient.

4. In the URL Address field, type the IP address you assigned to UST-IP in Step II-6. Press [ENTER] to load and launch the web access client.



Establish a Connection

Upon launching the Raritan Remote Client (RRC), UST-IP will request your user credentials. Log on with the default username and password (**admin** and **raritan**). You will connect to your UST-IP unit. Use the RRC Navigator, found on the left-hand side of the RRC window, to select and connect to a port.



Note to CommandCenter Users

If you are using UST-IP in a CommandCenter configuration, perform the installation steps as outlined above. After completing the steps in this chapter, please consult the CommandCenter user guide to proceed with your installation. The rest of this user guide applies primarily to users deploying UST-IP unit(s) without the integration functionality of CommandCenter.

Chapter 3: Raritan Remote Client

Invoking Raritan Remote Client (RRC) via Web Browser

UST-IP features Web Browser access, providing a connection from any Windows-based Remote PC running Microsoft Internet Explorer 4.0+, Mozilla 1.1+, and Netscape 7+.

Security Settings

Accessing UST-IP via web browser requires appropriate settings in the Internet Explorer security settings tab:

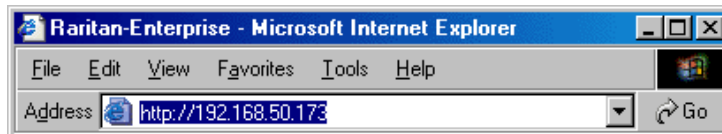
- “Download Signed ActiveX controls” should be set to either “Enable” or “Prompt”
- “Run ActiveX controls and plug-ins” should be set to either “Enable” or “Prompt”

Please consult your Microsoft Internet Explorer documentation for details regarding these settings.

Note: Microsoft Windows 2000 and Microsoft Windows XP restricts certain types of users from downloading and running ActiveX controls and plug-ins, regardless of the above settings in Internet Explorer. Please consult your Microsoft Windows documentation for more information.

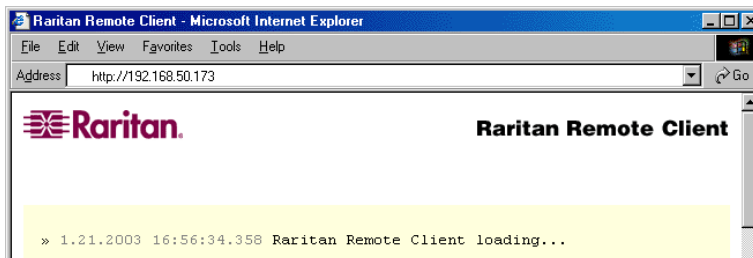
Launching Raritan Remote Client

1. After confirming that your browser security settings are configured appropriately, type the IP address assigned to your UST-IP unit (see **Chapter 2: Installation, Initial Configuration**) in the URL Address field of your web browser.

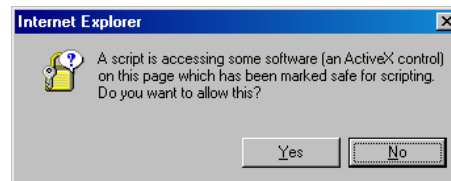
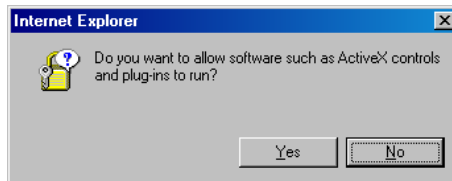


Note: UST-IP ships with the default IP address of 192.168.0.192

2. UST-IP redirects you to an HTTPS (128-bit) secure web page for launching RRC.



- Depending on your browser's security configuration, you may see any or all of the following dialog boxes, confirming the access and launch of an externally-provided program. Click **Yes** to advance through any of these prompts.



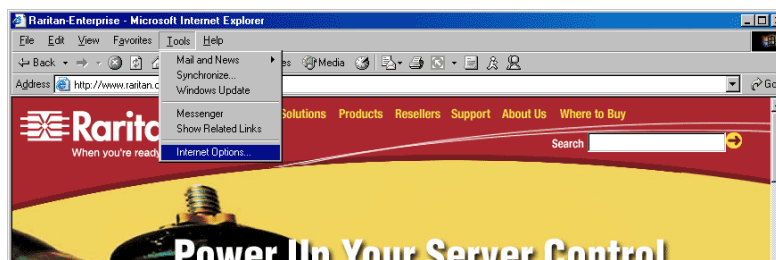
Note: Microsoft Windows 2000 and Microsoft Windows XP restrict certain types of users from downloading and running ActiveX controls and plug-ins, regardless of the settings in Internet Explorer and regardless of your approval of the above warnings. Please review the previous section, "**Security Settings**" and consult your Microsoft Windows documentation for more information.

Removing RRC from Browser Cache

To remove RRC from your browser cache, whether to perform an upgrade, save disk space, or remove evidence of RRC being executed on a PC, follow the standard procedure according to your web browser software.

Directions for Internet Explorer v6.0:

- If you have used RRC recently, exit and restart Internet Explorer.
- On the Internet Explorer menu bar, select **Tools → Internet Options**.



- When the **Internet Options** screen appears, click on the **Settings** tab, and then click on **View Objects**.
- Internet Explorer will display a list of cached program objects. Select any entries named **TeleControl Class** and delete them.

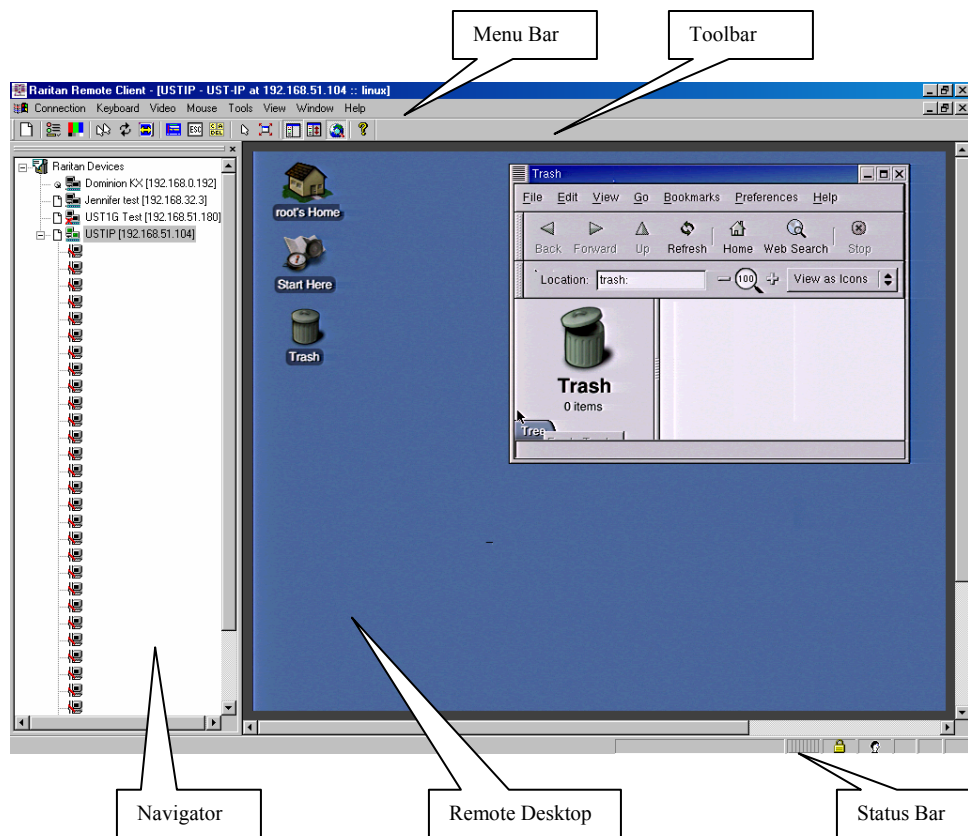
Optional: Installing Raritan Remote Client Software

Note: This step is optional. UST-IP can be accessed from a Remote PC either by installing RRC software, or by launching RRC via web browser (see previous section). Accessing UST-IP via web browser does not require any software installation on the Remote PC.

1. Insert the provided RRC CD-ROM into the CD-ROM drive of your PC.
2. The RRC setup program will run automatically. If it does not, right-click on your PC's CD-ROM drive in Windows Explorer and choose **Auto Play**.
3. Follow the on-screen instructions in the InstallShield Wizard to complete RRC installation on your Remote PC. Under "Select Components," you must select either the US version for a US Remote PC keyboard, or the Japanese version for a Japanese Remote PC keyboard.
4. Depending on the configuration of your PC, the RRC installation program may automatically install Direct X and Microsoft Foundation Class libraries if required. If this occurs, you will be directed to restart your PC upon completing installation.
5. A Raritan Remote Client icon will be added to your desktop. Click on this icon to launch RRC.

RRC Window Layout

Raritan Remote Client functions are grouped into five general sections on the screen. Each section will be discussed in detail further in this chapter.



RRC Navigator

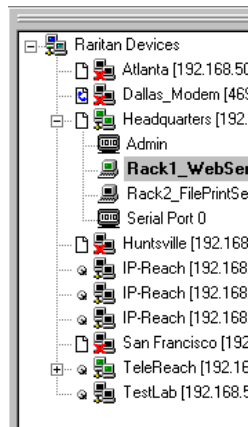
The RRC Navigator provides a single view to every known Raritan device, allowing convenient access to multiple Raritan networked appliances.

The RRC Navigator displays:

- All Raritan devices for which a *connection profile* exists
- All Raritan devices that are automatically identified on the network

Note: Automatic Raritan device identification uses UDP protocol, and will usually identify all Raritan devices on your subnet. Network administrators rarely allow UDP to function outside of a subnet.

Note: Automatic Raritan device identification will find only Raritan devices configured to use the default TCP Port (5000).



Note: Please refer to the Paragon II User Manual for further details on Paragon Tiering and Configurations.

Each device entry in the RRC Navigator provides two icons to communicate network status and connection profile information.

Left Icon (Connection Profile)

	Profiled – A network connection profile exists for this device.
	Modem Profile – A modem connection profile exists for this device.
	Not Profiled – RRC found this device on the network, but a connection profile does not exist for it.

Right Icon (Network Status)




	Connected (green) – You are currently authenticated and connected to this device.
	Available (black) – This device is currently available on the network, but you are not currently connected to it.
	Unavailable – A profile exists for this device, but it is not currently available on the network. (Note that all devices with modem profiles to which you are not currently connected will display this icon.)

For each Raritan device to which you are connected, the RRC Navigator expands its display tree to show each port for which you have access.

- Ports displayed with a green icon indicate that you are connected to that port.
- Bold type indicates which port is currently displayed (active) in the remote desktop area of the client.

Navigator Options

Certain RRC Navigator attributes may be customized to your preferences.

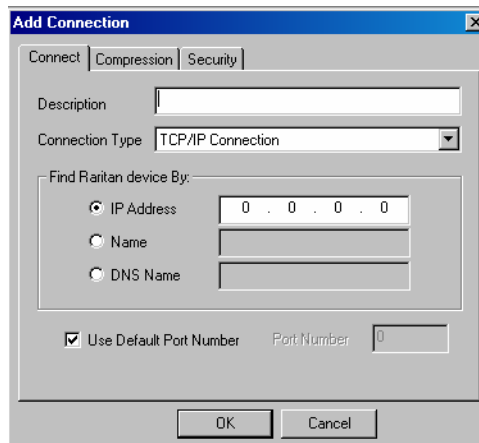
	Display / Hide Navigator – Toggle whether the RRC Navigator is shown. This option can also be toggled by choosing View → Navigator from the Menu Bar.
	Refresh Navigator – Update the device status information shown in the RRC Navigator.
	Show Browsed Devices – Toggle whether RRC Navigator should display "Not Profiled" devices automatically found on the network or show only devices for which profiles exist. This option can also be toggled by choosing View → All Devices from the Menu Bar.

Creating New Profiles

Connection profiles store important information about your Raritan device such as IP Address, custom TCP ports, preferred compression settings, and custom security keys.

To Create a Connection Profile:

1. Select **Connection** → **New Profile** from the Menu Bar, or click on the leftmost icon in the Toolbar. The Add Connection screen appears.



2. Type a text name that easily identifies the Raritan device that you are configuring in the **Description** field.
3. Click on the **Connection Type** drop-down arrow to select your connection type.
4. In the **Find Raritan device By:** panel, click on the radio button before your preference:
 - **IP Address:** The IP address assigned to your Raritan device (see **Chapter 4: Administrative Functions, Network Configuration**).
 - **Name:** The name assigned to your Raritan device during initial setup (see **Chapter 4: Administrative Functions, Network Configuration**).

Note: If dynamic DHCP addressing is used for UST-IP, use "Find UST-IP by Name."

Note: The factory default unit name for each UST-IP is **UST-IP**. To change the default name on a UST-IP unit and institute a unique name, see **Chapter 4: Administrative Functions**.

- **DNS Name:** If you have configured your DNS server to resolve a DNS name to the IP address that you have assigned to your Raritan device, use this DNS name to access your Raritan device.

For a Dial-Up Connection, enter the dialing parameters that RRC should use to establish a connection:

- **Phone Number:** Be sure to include any additional codes that RRC should dial to establish a connection (country codes, area codes, outside line access codes, etc.)

- **Modem:** Select the modem, as configured in Windows, which RRC should use to dial and connect to your Raritan device.

Select a TCP Port to use:

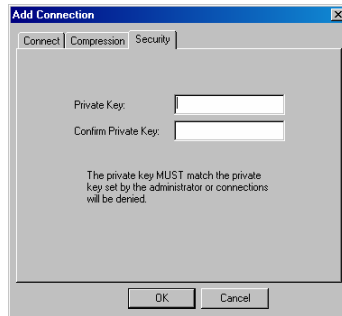
- **Use Default Port Number:** UST-IP is configured by default to use TCP Port 5000 for communicating with RRC. UST-IP can be configured to use a different TCP Port (see **Chapter 4: Administrative Functions, Network Configuration**); if so, uncheck the **Use Default Port Number** option, and enter the configured TCP Port to be used.

5. Other tabs on this screen include:

Compression Tab

Settings in the Compression Tab are adjustable via the RRC client, and therefore are not necessary for pre-configuration in the Connection Profile. Should you wish to pre-configure these settings, however, refer to the section in this chapter labeled, **Connection and Video Properties**.

Security Tab



The screenshot shows a dialog box titled "Add Connection" with three tabs: "Connect", "Compression", and "Security". The "Security" tab is active. It contains two text input fields: "Private Key:" and "Confirm Private Key:". Below the fields is a warning message: "The private key MUST match the private key set by the administrator or connections will be denied." At the bottom of the dialog are "OK" and "Cancel" buttons.

If you have configured your UST-IP unit to use a private group key, you must enter it here in order to be authorized to initiate a connection with that UST-IP unit. Click [**OK**] when you have completed the fields.

When you have completed the Connect and Security screens, click [**OK**] to finish creating the connection.

Establishing a New Connection

To connect to a Raritan networked device, simply double-click on its entry in the RRC Navigator. You will be asked to authenticate the device.

***Note:** The default UST-IP login user name is **admin**, with the password **raritan**. This user has administrative privileges. Passwords are case sensitive and must be entered in the exact case combination in which they were created. The default password **raritan** must be entered entirely in lowercase letters. To ensure security, change the default username password as soon as possible.*

If you do not see an entry for your UST-IP in the RRC Navigator, follow the instructions in the **Creating New Profiles** section in this chapter to create a new connection profile for your UST-IP.

If you are having problems connecting to a Raritan device, be sure to check the following:

- **Username / Password:** Raritan usernames and passwords are case-sensitive.
- **TCP Port:** If you have configured your Raritan Device to use a non-default TCP Port, this information must be entered into its connection profile.
- **Firewall Settings:** If you are accessing a Raritan Device through a firewall, that firewall must be configured to allow two-way communication on TCP Port 5000 (or the custom TCP Port to which your Raritan Device has been configured).
- **Security Key:** If you have configured your Raritan Device to require a group security key, that key must be entered into the device's connection profile.
















Closing a Remote Connection

When you would like to terminate your connection to an UST-IP unit, simply right-click on the device entry in the RRC Navigator, and select **Disconnect**.

RRC Toolbar and Shortcuts

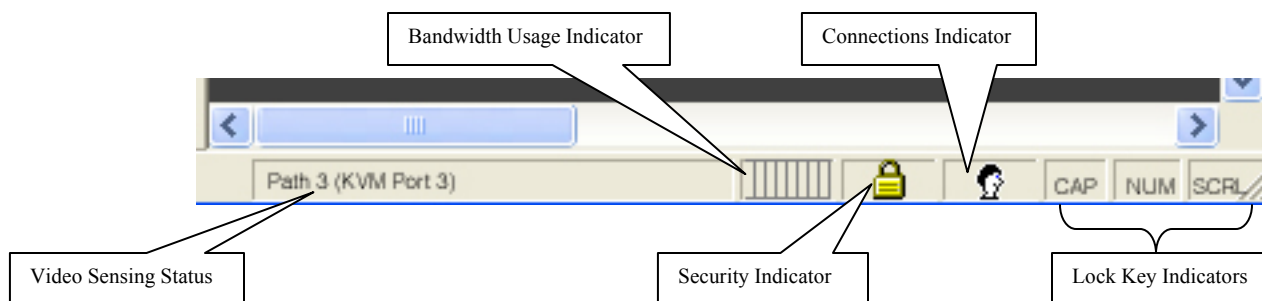


The RRC Toolbar provides convenient, one-click access to the most commonly used features and parameters of Raritan Remote Client:

BUTTON	BUTTON NAME	HOTKEY	FUNCTION
	New Profile	<Ctrl+Alt+C>	Creates a new Navigator entry for a Raritan device; same results as selecting Connection → New Profile in the menu bar.
	Connection Properties	<Ctrl+Alt+P>	Opens Modify Connection Properties dialog box to manually adjust bandwidth-correlated options (Connection Speed, Color Depth, etc.).
	Video Settings	N/A	Opens the Video Settings dialog box to manually adjust video conversion parameters.
	Synchronize Mouse	<Ctrl+Alt+S>	In dual-mouse mode, forces realignment of target server mouse pointer with Raritan Remote Client mouse pointer.
	Refresh Screen	<Ctrl+Alt+R>	Forces refresh of video screen.
	Auto-sense Video Settings	<Ctrl+Alt+A>	Forces refresh of video settings (resolution, refresh rate).
	Enter On-Screen Menu	N/A	Not applicable for UST-IP. Used by RRC with other Raritan products.
	Exit On-Screen Menu	ESC	Not applicable for UST-IP. Used by RRC with other Raritan products.
	Send Ctrl+Alt+Del	<Ctrl+Alt+D>	Sends a Ctrl+Alt+Del key sequence to the target server.
	Single Cursor Mode	<Ctrl+Alt+X>	Enters Single Cursor Mode, in which the local PC's mouse pointer no longer appears on-screen. Press <Ctrl+Alt+X> to exit this mode.
	Full Screen Mode	<Ctrl+Alt+F>	Maximizes the screen real estate to view the target server desktop.
	Show / Hide Navigator	N/A	Toggles whether or not the RRC Navigator is displayed.
	Refresh Navigator	N/A	Forces a refresh of the data displayed by the RRC Navigator.
	Show / Hide "Browsed" Devices	N/A	Toggles whether or not the RRC Navigator displays Raritan Devices automatically identified on the network (that do not have pre-configured profiles associated with them).
	About	N/A	Displays version information about Raritan Remote Client.

RRC Status Bar

The **Status Bar** at the bottom of the Raritan Remote Client window conveys information about the status of your remote connection session to UST-IP.



Video Sensing Status

Indicates the occurrence of video sensing that reflects a counter until the video actually appears. This matches what the user sees on the screen.

Bandwidth Usage Indicator

Indicates how much of your total available bandwidth is currently being used. The **Connection Speed** setting, found under the Compression tab of the Connection Properties screen, determines total available bandwidth.

Security Indicator

Indicates whether the current remote connection is protected by encryption. Encryption requirements are set during UST-IP configuration (see **Chapter 4: Administrative Functions**). When an UST-IP device is configured for **No encryption** or **SSL Authentication, NO data encryption**, the Security Indicator is represented on the Status Bar as an open lock. When **SSL authentication, data encryption** or **SSL authentication, SSL encryption** is selected, the Security Indicator is represented on the Status Bar as a closed lock.

Connections Indicator

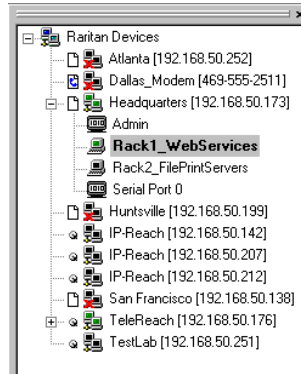
Indicates whether you have a local or remote user present. If there is no other user present, you will not see this icon.

Lock Key Indicators

Indicates the status of the current Target Server, with respect to the activation of the Caps-Lock, Num-Lock, and Scroll-Lock keys. If these keys are enabled on the Target Server being viewed, this affirmative status will be reflected on the Status Bar as indicated.

Remote KVM Console Control

After using the RRC Navigator to establish a connection with an UST-IP unit (see the previous section: **Establishing a New Connection**), the Navigator entry corresponding to the UST-IP unit will expand to show all ports on the UST-IP enabled for remote access.

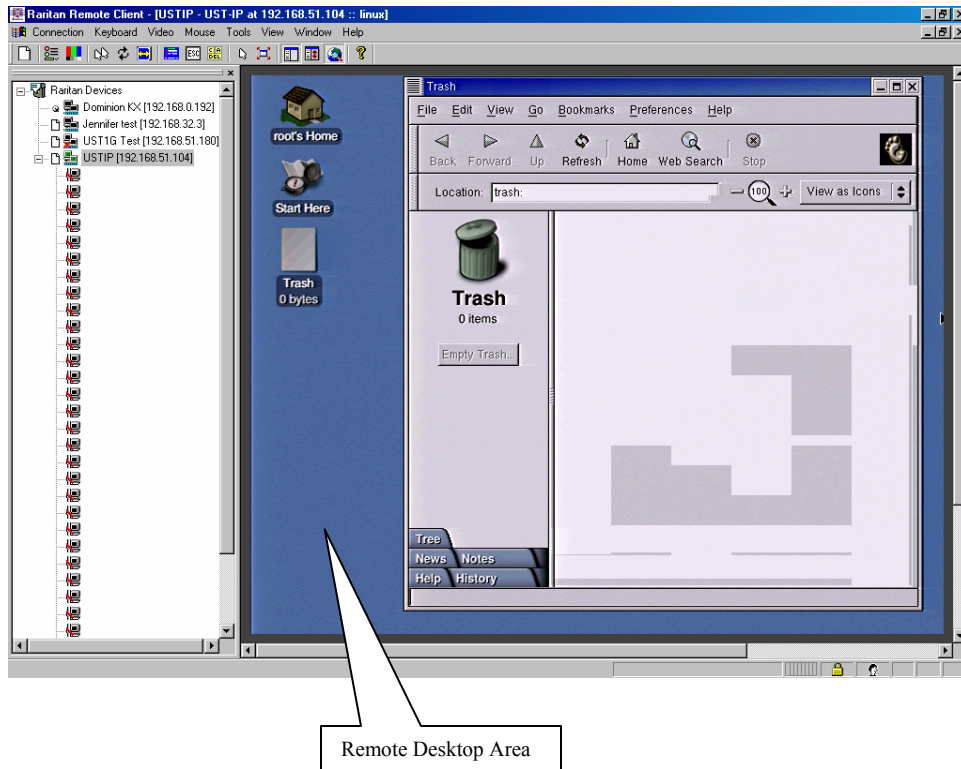


To establish a remote KVM console connection, simply double-click on the KVM path that you would like to control.

Upon connection, UST-IP displays the real-time video output by the KVM switch or server that is connected to your UST-IP KVM port. This video is compressed and encrypted according to the configuration settings specified by the administrator (see **Chapter 4**).

Once connected to a KVM switch or a server, you obtain complete, low-level control of the KVM console as if you were physically located next to the KVM switch or server.

When your mouse pointer lies within the Remote Desktop area of RRC, mouse movements and clicks are transmitted to the KVM switch or remote server connected.



Single Mouse Mode / Dual Mouse Mode

When remotely viewing a Target Server that uses a pointing device, by default you will see two mouse pointers within the Remote Desktop area of the Raritan Remote Client window. The Raritan Remote Client mouse pointer, generated by the operating system on which RRC is running, slightly leads the Target Server's mouse pointer during movement, a necessary result of digital delay.

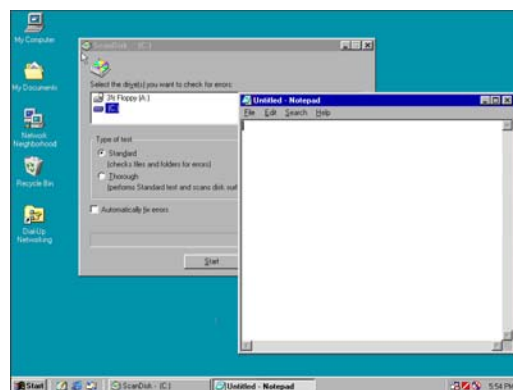
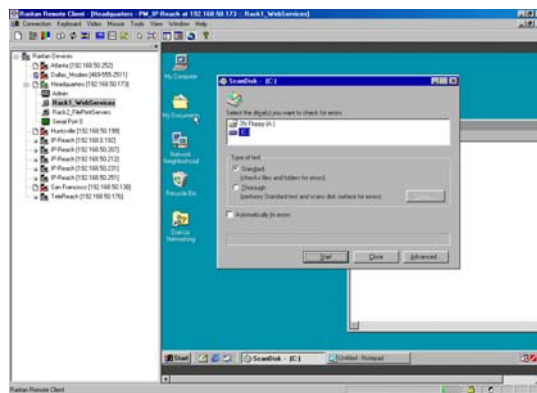
On fast LAN connections, however, some users prefer to disable the Raritan Remote Client mouse pointer, opting to view only the Target Server's mouse pointer during operation. To toggle between these two modes, use the <Ctrl+Alt+X> hotkey, or press the **Single Mouse Pointer** mode icon in the RRC Toolbar.

***Note:** For better alignment between the two mouse pointers in dual-mouse mode, click **Synchronize Mouse** button on the RRC Toolbar, or simultaneously press the keys **Ctrl+Alt+S**. This forces a realignment of the two mouse pointers. If you have carefully followed the **Configuring Target Servers** directions found in Chapter 2, and the mouse pointers still remain out of sync, click on the **Auto-Sense Video** button on the RRC Toolbar.*

Full Screen Mode

Raritan Remote Client's full screen mode maximizes the screen real estate available to RRC for displaying the remote desktop by removing window borders, toolbars, status bars, and the RRC Navigator.

This option is particularly useful for viewing a Target Server whose video resolution is equal to or greater than the video resolution setting of the PC on which RRC is running, for example, viewing a 1024x768 server on a 1024x768 PC.



To toggle full screen mode, click on the full screen mode icon in the RRC Toolbar (or press the hotkey combination **Ctrl+Alt+F**). To exit full screen mode, press the hotkey combination **Ctrl+Alt+F**.


Keyboard Macros

RRC allows users to create custom keyboard macros in order to send given key sequences to the remote server or KVM switch connected to UST-IP. This feature allows customers to send keystrokes to remote servers that may be otherwise unintentionally interpreted by the computer on which RRC is running.

UST-IP's Keyboard Macro feature can be used to ensure that keystroke combinations intended for the Target Server are sent to, and interpreted only by, the Target Server.

Ctrl+Alt+Delete Macro

Due to its frequent use, a Ctrl+Alt+Delete macro has been pre-programmed into Raritan Remote Client, and is useful in illustrating the power of keyboard macros.

	Send Ctrl+Alt+Del	Ctrl+Alt+D	Sends a Ctrl+Alt+Delete macro to the Target Server.
---	----------------------	-------------------	---

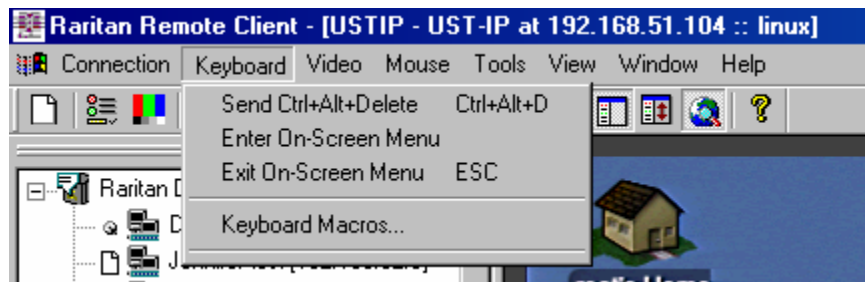
Clicking on the Ctrl+Alt+Delete icon in the RRC Toolbar sends this key sequence to the server or KVM switch to which you are currently connected. In contrast, if you were to physically press the Ctrl+Alt+Delete keys while using RRC, the command would first be intercepted by your own PC due to the structure of the Windows operating system, instead of sending the key sequence to the target server as intended.

Building a Keyboard Macro

To illustrate the creation of a keyboard macro, the following directions detail the steps necessary to create a keyboard macro for the Windows command, "Minimize All Windows / Show Desktop".

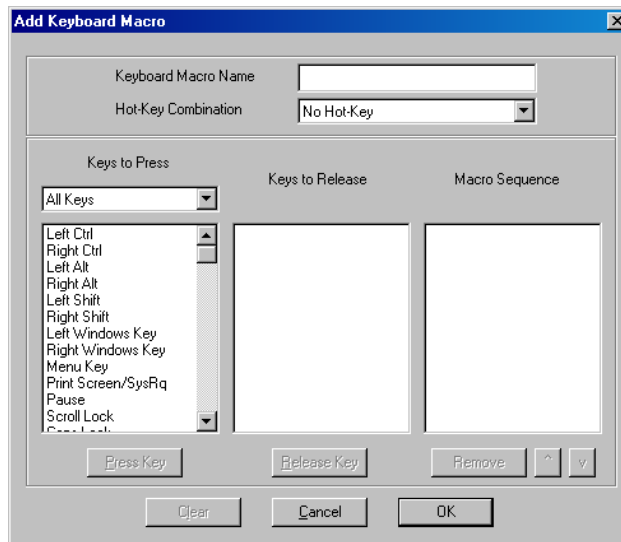
In Windows, pressing the **Windows+D** key combination minimizes all program windows. However, when connected to a target server with RRC, a keyboard macro is the only means to accomplish this task on the target server – because, again, pressing the key combination **Windows+D** would result in your own client PC intercepting the command and performing it – instead of sending the command to the target server as intended.

1. On the RRC Menu Bar, select **Keyboard → Keyboard Macros**.

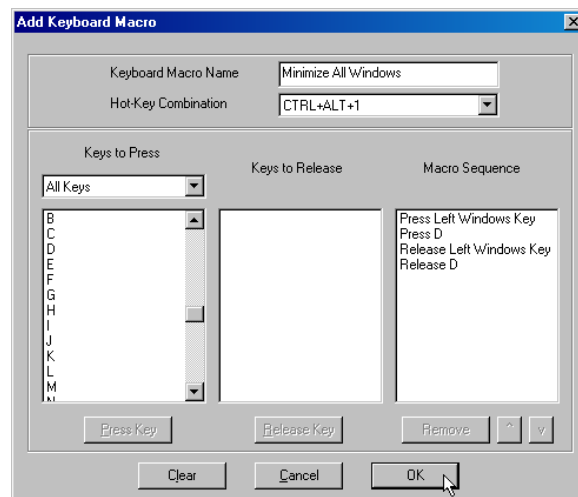


2. When the Keyboard Macros dialog box opens, click **Add**.

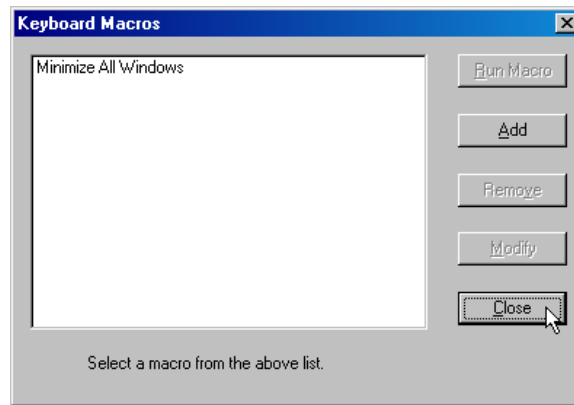
3. The Add Keyboard Macro dialog box opens.



4. Build the Keyboard Macro by editing all the fields in the Add Keyboard Macro window, in the order described below. Click **OK** when finished.
 - a. Enter a name into the **Keyboard Macro Name** field, which will appear on the RRC Menu Bar, after successful creation of the keyboard macro. For our example, "Minimize All Windows".
 - b. **Optional:** Designate a keystroke combination in the **Hot-Key Combination** field, which allows easy macro execution from your keyboard when RRC is running. For our example "Minimize All Windows," we selected **Ctrl+Alt+1**.
 - c. In the **Keys to Press** selection box, select each key for which you would like to emulate key presses – in the order by which they are to be pressed – clicking **Press Key** after each selection. As each key is selected, it will appear in the **Keys to Release** selection box in the middle of the dialog box.
 - In our "Minimize All Windows" example, we require the transmission of two keys: the **Windows** key and the letter **D** key.
 - d. In the **Keys to Release** selection box, select each key for which you would like to emulate key releases – in the order by which they are to be released – clicking **Release Key** after each selection.
 - In our "Minimize All Windows" example, we require both keys pressed to also be released.
 - e. Review the **Macro Sequence** text box, whose contents are automatically generated, to ensure that the contents accurately reflect the exact key sequence you desire. Use the **Remove** and the arrow buttons to adjust the contents and order of your macro if necessary.



5. After clicking **OK**, the Keyboard Macros dialog box will appear, listing your new keyboard macro.



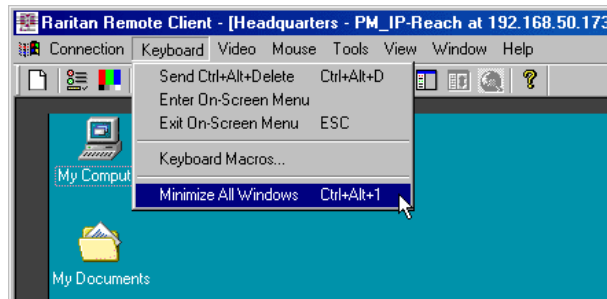
6. Click **Close** to complete the keyboard macro editing procedure.

Running a Keyboard Macro

Once a macro is created, it can be run via the RRC Menu Bar or with the hotkey combination if one had been designated during the macro creation.

Menu Bar Activation

After a macro has been created, it appears in the Keyboard menu on the RRC Menu Bar. You can simply click on the entry to execute your new keyboard macro.



Hot-Key Activation


Alternatively, once a macro has been created, it can be executed while using RRC by pressing the hotkey you (optionally) assigned to the macro. In the “Minimize All Windows” example described above, a user can press the keys **Ctrl+Alt+1** simultaneously while using RRC to send the **Windows+D** key combination to the target server.

Connection and Video Properties

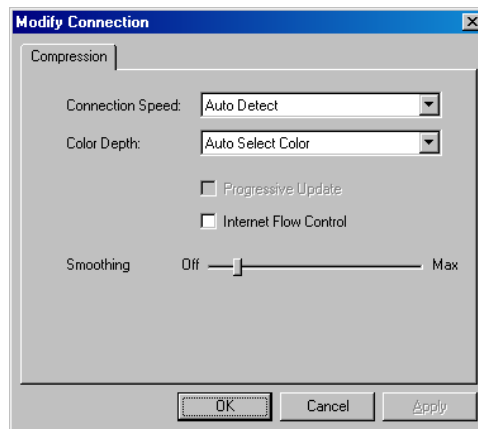
UST-IP's dynamic video compression algorithms maintain KVM console usability under varying bandwidth constraints. Unlike competitive solutions, UST-IP optimizes its KVM output for not only LAN utilization, but also via the WAN and dial-up. By dynamically adjusting color depth and limiting video output, UST-IP offers the optimal balance between video quality and system responsiveness in any bandwidth constraint.

Power users of RRC should understand the following adjustable parameters in the **Connection Properties** and **Video Settings** dialog boxes, and familiarize themselves with the effects of each setting – in different operating environments; they can be optimized to your requirements.

Connection Properties

	Connection Properties	<Ctrl+Alt+P>	Opens Modify Connection Properties dialog box to manually adjust bandwidth-correlated options (Connection Speed, Color Depth, etc.).
---	-----------------------	--------------	--

To access the Connection Properties dialog box, either select **Connection** → **Connection Properties** from the RRC Menu Bar, or click the **Connection Properties** shortcut button in the RRC Toolbar.



Connection Speed

The Connection Speed selection box allows users to manually constrain UST-IP from using more than a designated amount of network bandwidth. While UST-IP normally automatically detects available bandwidth, users can use the Connection Speed setting to manually inform UST-IP of a bandwidth constraint – whereby UST-IP adapts its behavior and simply refrains from even attempting to consume more than the available bandwidth.

Color Depth

For most administrative tasks (server monitoring, reconfiguring, etc.), server administrators do not require the full 24-bit or 32-bit color spectrum made available by most modern video graphics cards. Attempting to transmit such high color depths, then, would waste an enormous amount of precious network bandwidth.

Instead, UST-IP can dynamically adapt the color depth transmitted to remote users, in order to maximize usability in all bandwidth constraints.

- **Progressive Update** option: The extremely innovative UST-IP feature of Progressive Update can enormously increase usability in constrained bandwidth environments. When Progressive Update is enabled, UST-IP first sends an image of the remote desktop at lower color depths, and then provides higher color depth images as bandwidth allows.

This option is very similar in philosophy as the common World Wide Web notion of "interlaced GIF" files.

Note: When Color Depth is set to Auto Select Color (default), Progressive Update is automated. UST-IP will enable/disable Progressive Update as needed, disabling it for fast connections and enabling it for slow connections.


Internet Flow Control

Many public WAN links are by their very nature unpredictable. Packets sent over the public Internet do not necessarily arrive at their destination in the order they were sent. When using UST-IP over an unpredictable public WAN (particularly in international scenarios), the Internet Flow Control toggle ensures that packets transmitted by UST-IP are received and reconstructed by RRC in the correct order.

Smoothing

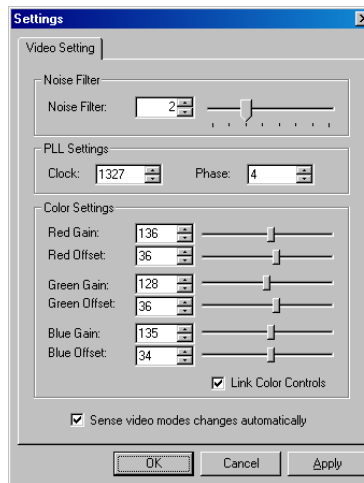
The video smoothing level instructs UST-IP to what degree color gradation shifts are relevant for transmission. Video pixels that stray from the majority color are assigned approximated color values to reduce bandwidth used and video noise transmitted. Overly high smoothing levels can result in color inaccuracies; whereas lower smoothing levels require greater bandwidth and processing power.

Video Settings

	Video Settings	N/A	Opens the Video Settings dialog box to manually adjust video conversion parameters.
---	----------------	-----	---

To access the Video Settings dialog box, either select **Video → Video Settings** from the RRC Menu Bar, or click on the [**Connection Properties**] button in the RRC Toolbar.

Most of the settings in this dialog box can be refreshed by performing Color Calibration, as described in the next section, or by manually forcing UST-IP to auto-detect the video settings (on the RRC Menu Bar, select **Video → Auto-sense Video Settings**). However, it is useful for power users to understand the meanings and ramifications of each setting.



Noise Filter

The video output of graphics cards are transmitted in analog form, and are susceptible to electrical and interference noise. UST-IP's advanced circuitry can filter out these small, false, and unintended signal variations, thereby optimizing picture quality and bandwidth consumed.

Higher: Noise Filter settings instruct UST-IP to transmit a variant pixel of video only if a large color variation exists in comparison to its neighbors. However, setting the threshold too high can result in the unintentional filtering of desired screen changes.

Lower: Noise Filter settings instruct UST-IP to transmit most pixel changes. Setting this threshold too low results in higher bandwidth utilization.

Note: Lower Noise Filter settings (approximately 1 to 4) are recommended. Although higher settings will stop the needless transmission of false color variations, true and intentional small changes to a video image may not be transmitted.

Analog-to-Digital Settings

The following parameters are best left to UST-IP to automatically detect (on the RRC Menu Bar, select **Video > Auto-sense Video Settings**), but a brief description of each is included here.

- **PLL Settings:** If the video image looks extremely blurry or unfocused, the PLL Settings for clock and phase can be adjusted until a better image appears on the active Target Server.
 - **Clock:** Horizontal sync divider to produce pixel clock. Controls how quickly video pixels are displayed across the video screen. Changes made to clock settings cause the video image to stretch or shrink horizontally. Odd number settings are recommended.
 - **Phase:** Phase values range from 0 to 31 and will wrap around. Stop at the phase value that results in the best video image for the active Target Server.
- **Color Settings:** Gain control can be thought of as contrast adjustment. Offset control can be thought of as brightness adjustment.
 - **Red Gain:** Controls the amplification of the red signal.
 - **Red Offset:** Controls the bias of the red signal.
 - **Green Gain:** Controls the amplification of the green signal.
 - **Green Offset:** Controls the bias of the green signal.
 - **Blue Gain:** Controls the amplification of the blue signal.
 - **Blue Offset:** Controls the bias of the blue signal.
 - **Link Color Controls:** Makes all gain slide adjusters move in unison when any one color's gain slide is moved and all the offset slide adjusters move in unison when any one color's offset slide is moved.
- **Sense video mode changes automatically:** Determines whether UST-IP will automatically update the video image being sent RRC each time it detects a change in video resolution or refresh rates at the Target Server.

Note: Please refer to the Paragon II User Manual for further details on Video Settings.

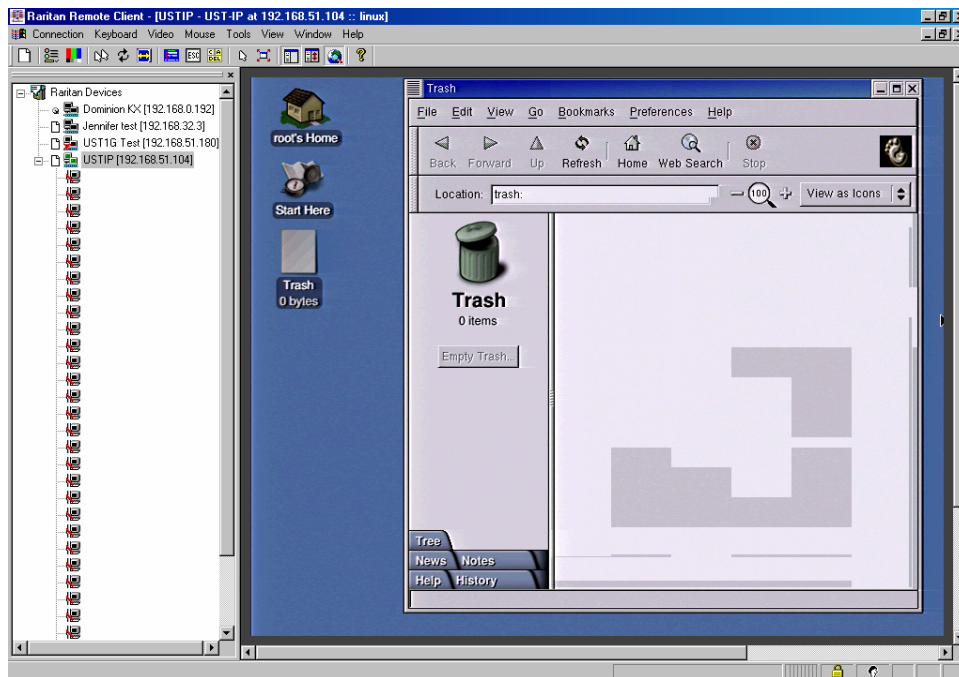
Color Calibration

Automatic Color Calibration adjusts the color settings on UST-IP to reduce excess color noise and data during digitization of video images. This data streamlining will increase the operational performance of UST-IP, particular color accuracy.

A very simple procedure to execute, Color Calibration should be performed if the color levels (hue, brightness, saturation) of transmitted video images do not seem accurate. Because UST-IP color settings remain static and do not change when switching from one Target Computer to another, performing this Color Calibration routine once on a single representational Target Server will benefit all connected Target Servers.

To Perform Color Calibration:

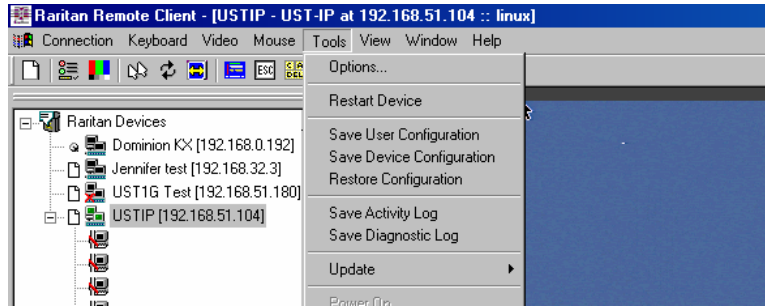
1. Open a remote KVM connection to any server running a graphical user interface.
2. Ensure that a solid white color covers approximately 15% or more of the target server's desktop. One simple way to accomplish this is to open the Notepad application and maximize its window size.



3. On the RRC Menu Bar, select **Video** → **Calibrate Color** to perform the color calibration.

Remote Device Administration

When logged into an UST-IP unit as a user with administrative privileges, UST-IP allows you to perform many powerful device administration tasks remotely.



Configuration Menus

An Administrative user can access UST-IP's lowest level configuration menus (explained in detail in [Chapter 4](#)), by double-clicking the "Admin" port entry of an UST-IP device shown in the RRC Navigator.

Firmware Upgrade

Remote firmware upgrades may be performed by selecting **Tools → Update Device** on the RRC Menu Bar. RRC will prompt you to locate a Raritan firmware distribution file (*.RFP format), which can be found on the Raritan web site (www.raritan.com) when available. Be sure to read all instructions included in firmware distributions before performing an upgrade.

Device Restart

Administrative users may restart UST-IP units by selecting **Tools → Restart Device** on the RRC Menu Bar.

Device Configuration Backup and Restore

By selecting **Tools → Save Device Configuration** and **Tools → Restore Device Configuration** on the RRC Menu Bar, Administrative users may download and upload complete UST-IP configurations to their local computers for archiving.

Log Files

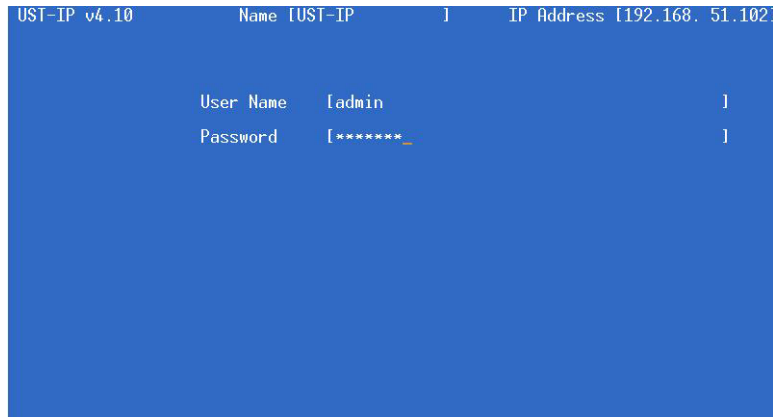
UST-IP provides detailed activity logs for troubleshooting purposes, which may be downloaded to your local computer for viewing, reporting, and analysis. On the RRC Menu Bar, select **Tools → Save Activity Log**, or **Tools → Save Diagnostic Log**.

Chapter 4: Administrative Functions

Accessing the Administrative Functions

Access and execute Administrative functions via local admin console, or via remote administration. Only administrators (users with administrative privileges) can access the UST-IP Administrative Menus.

Local Admin Console



Power ON the UST-IP unit via the power switch on the back of the unit.

*Note: The default UST-IP login user name is **admin**, with the password **raritan**. This user has administrative privileges. Passwords are case sensitive and must be entered in the exact case combination in which they were created. The default password **raritan** must be entered entirely in lowercase letters. The password cannot be changed from USTIP. When connected to a UMT, it will adopt the UMT's administrator password.*

Important: The UST-IP Administration menus shown here administer only UST-IP settings, not Paragon settings.

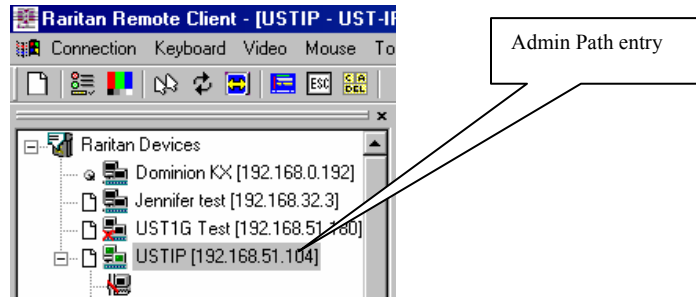
Remote Admin Console

An alternative way to access UST-IP's administrative functions is to do so remotely, using the Raritan Remote Client.

Any administrative user logged on to UST-IP at a Remote PC can perform administrative functions remotely to make changes to the system, as long as UST-IP is set to allow remote administration privileges – see Allow Remote Administration on the Security Configuration screen.

Note: Only users with administrator privileges can access the Remote Admin feature.

To access the Administrative menus from Raritan Remote Client, double click on the Admin path entry displayed on the RRC Navigator for the UST-IP unit you wish to configure.



Navigating the Administrative Menus

```

UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.104]

- Main Menu -

[C] Configure UST-IP
[V] View UST-IP status
[R] Restart or shutdown the UST-IP
[D] Diagnostics

Press TAB to move to an option and ENTER to select the option.

```

- Use the **Tab**, **↑**, **↓**, or **C** keys on your keyboards to highlight the **Configure UST-IP** selection, then press the **Enter** key. You may need to reboot.
- Press **Ctrl+S** to save changes. **You must press Ctrl+S before exiting any screen you have changed.**
- Use the **Tab**, **↑**, **↓** or **N** keys to highlight the **Network Configuration** selection, then press the **Enter** key.

```

UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.104]

- Configuration Menu -

[N] Network Configuration
[U] User Station Options
[S] Security Configuration
[P] Performance Settings
[T] Time and Date
[A] Access Control List
[L] Remote Syslog
[M] Return to the main menu

Press TAB to move to an option and ENTER to select the option.

```

Network Configuration

Please note that after you have made changes to the Network Configuration, you must press **Ctrl+S** to save your changes. Reboot after all changes are saved to apply them to your Network.

```

UST-IP v4.1.0      Name [UST-IP      ]      IP Address [192.168. 51.104]
- Network Configuration -

Name              [UST-IP      ]
Enable Ethernet Interface [YES]
Line Speed & Duplex [Auto Detect ]
Obtain IP address automatically (DHCP) [NO ]
IP Address        [192.168. 51.104]
Subnet Mask       [255.255.255. 0 ]
Default Gateway   [192.168. 51.126]

Enable Modem Interface [NO ]
Enable Web Browser Interface [YES]
Use Default TCP Port 5000 [YES]

CTRL+S - Save Changes  ESC - Cancel Changes  TAB - Next Field

```

- **Name:** Designate a unique name for this UST-IP unit, for example, “Miami Data Center.” The default name is UST-IP.
- **Enable Ethernet Interface:** Designates whether UST-IP should enable its Ethernet adapter as active (default: YES).

Note: Network connections must be 10BASE-T or 100BASE-TX Ethernet

- **Line Speed & Duplex:** Auto detect 10 Mbps/Full Duplex, 10 Mbps/Half Duplex, 100 Mbps/Full Duplex, or 100 Mbps/Half Duplex
- **Obtain IP address automatically (DHCP):**
 - ◆ **YES:** Enables dynamic IP addressing for UST-IP. Each time UST-IP boots, it will request an IP address from the local DHCP server. Note that this setting can make remote access to UST-IP from outside the LAN difficult, since the dynamically assigned IP address must be known in order to initiate a connection.
 - ◆ **NO (default):** Assigns a fixed IP address to the UST-IP unit (recommended).
 - **IP Address:** Enter the IP address for UST-IP given by your Network Administrator.
 - **Subnet Mask:** Enter a Subnet Mask provided by your Network Administrator.
 - **Default Gateway:** Enter the Default Gateway if your Network Administrator specifies one.
- **Enable Modem Interface:** Enables Dial-up Modem access (default: YES). For UST-IP, an external serial modem must be connected in order for this function to work properly.
- **Enable Web Browser Interface:** Enables web browser access to UST-IP (default: YES).
- **Use Default TCP Port 5000:**
 - **YES (default):** Utilizes the default port 5000.
 - **NO:** Enter an alternate port number.

Note: In order to access UST-IP from beyond a firewall, your firewall settings must enable two-way communication through the default port 5000, or the non-default port configured above.

User Station Options

In the User Station Configuration screen, use the ← and → arrows on your keyboard to set **Port Priority** to favor **None**, **Remote**, or **Local** users:

- If you set Port Priority to **Remote**, a Remote user will automatically terminate a Local user session when attempting to connect to the same USTIP unit.
- If you set Port Priority to **Local**, a Local user will automatically terminate a Remote user session when attempting to connect to the same USTIP unit.
- If you set Port Priority to **None**, there is no capability to automatically terminate a user session. Instead, the user, regardless of Remote or Local status, who connects first to the port will have access to the port until the user terminates the session. If a port is occupied, a message appears to any other users attempting to gain access, to inform them of port status.

```

UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.104]
- UserStation Configuration -

Port Priority      [NONE      ]

Press SPACE BAR to toggle the options.

CTRL+S - Save Changes  ESC - Cancel Changes  TAB - Next Field

```

Security Configuration

```

UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.104]
- Security Configuration -

Encryption mode    [SSL authentication, data encryption ]
Allow remote administration [YES]
Logout idle users  [Never      ]
Private key        [          ]
Confirm private key [          ]

Enable SNMP        [NO ]

Press SPACE BAR to toggle the options.

CTRL+S - Save Changes  ESC - Cancel Changes  TAB - Next Field

```

- **Encryption mode:** Toggle through the choices and select the desired level of encryption for initial connection authentication and remote session video data transfer.
 - **No encryption:** No encryption or security. Neither the initial connection authentication nor remote video data transfer is encrypted.
 - **SSL authentication, NO data encryption:** This mode secures user names and passwords, but not KVM data. 128-bit Secure Socket Layer (SSL) protocol provides a private communications channel between UST-IP and the Remote PC during initial connection authentication. No encryption security in place during remote KVM data transfer.
 - **SSL authentication, data encryption (default):** This mode secures user names, passwords, and KVM data. 128-bit Secure Sockets Layer (SSL) protocol provides a private communications channel between UST-IP and the Remote PC during initial connection

authentication. After authentication, KVM data is also transferred with 128-bit encryption, but using a proprietary protocol more efficient than SSL.

- **SSL authentication, SSL data encryption:** This mode secures user names and passwords, and provides high-level security for KVM data. 128-bit Secure Sockets Layer (SSL) protocol provides a private communications channel between UST-IP and the Remote PC during initial connection authentication. 128-bit SSL encryption is also in place during remote KVM data transfer.

***Note:** SSL data encryption increases the amount of data that must be sent over the remote connection, and is, therefore, not recommended for modem or very slow Internet connections. The default setting “SSL authentication, data encryption” offers exactly the same level of security with a higher level of efficiency.*

- **Allow remote administration:**
 - **NO:** To keep access to all Administrative Functions available only from the UST-IP Admin Console, and not from a Remote PC.
 - **YES (default):** Allows remote access to all Administrative UST-IP Functions by administrators logged on at a Remote PC.
- **Logout idle users:** Offers an option for UST-IP to automatically disconnect remote users after certain selected time intervals of inactivity have passed.
 - **Never (default):** Idle remote users will never be disconnected.
 - **After 5, 15, 30, 60, or 120 minutes:** Idle remote users will be automatically disconnected from UST-IP after the selected time period has passed with no active input from the Remote PC.
- **Private key:** Enter a private key password. This private key acts as a second level of password protection. Only remote users who know the private key password, in addition to their user name and password, can log in and connect to UST-IP.
 - **Confirm private key:** Enter private key password again for re-confirmation.
 - **Configure private key:** You must perform the following steps to create a private key password.
 1. Press TAB to advance to the Private key field and type a Private Key number; the Private Key can be up to 23 alphanumeric characters. Do not use special characters, such as # or \$ (if special characters are included, the Private Key will fail).
 2. Press TAB once and retype the Private Key in the Confirm private key field.
 3. Press CTRL+S on your keyboard to save the Private Key. A confirmation message appears.
 4. Restart the UST-IP device to save the Private Key on your server. Please note that rebooting the UST-IP should take approximately 60 seconds, but may take longer, depending on your Paragon configuration.

In order for the private key functionality to work correctly after you have rebooted the UST-IP device, you must modify the UST-IP profile in the Raritan Remote Client (RRC). Please perform the following steps:

1. After you have reconnected to the RRC, scroll down in the Navigator window and right-click on the UST-IP icon.
2. Click **Modify Profile** in the shortcut menu.
3. Click on the **Security** tab.
4. Type the Private Key you just entered in the **Private Key** field of the UST-IP Security Configuration menu.
5. Retype the Private Key in the **Confirm Private Key** field.
6. Click **OK** to save the Private Key to the UST-IP profile.

You may now log onto your UST-IP device remotely through the RRC.

***Note:** Private key passwords are case sensitive. For remote user login, they must be entered by the user in the exact case combination in which they were created here.*

***Note:** Private key passwords must be alphanumeric. Special characters cannot be used.*

- **Enable SNMP:** Toggles whether UST-IP responds to SNMP GET REQUESTS

Performance Settings

The Performance Settings screen is used to set up UST-IP's video data transfer and bandwidth parameters.

```

UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.104]

- Performance Settings -

Pause video stream for idle users      [After 120 minutes]

Maximum total Bandwidth usage          [No Limit   ]
Maximum Bandwidth per user            [No Limit   ]

NOTE: Limiting Bandwidth usage will affect video performance.

Press SPACE BAR to toggle the options.

CTRL+S - Save Changes  ESC - Cancel Changes  TAB - Next Field

```

- **Pause video stream for idle users:** Pausing the flow of video data during periods of prolonged inactivity will prevent an inactive user from needlessly consuming bandwidth.
 - **Never (default):** Video data will continually be sent to Remote PC, constantly updating the screen, even if the remote user is Idle, sending no active input to UST-IP.
 - **After 5, 15, 30, 60, or 120 minutes:** Video data flow to the Remote PC will pause after the selected time period has passed with no active input from the Remote PC.
- **Maximum total Bandwidth usage:** Sets an upper limit to the amount of bandwidth that can be consumed by this one UST-IP unit.
 - **No Limit (default):** UST-IP can consume as much bandwidth as needed.
 - **10, 5, 2, or 1 megabit or 512, 256, 128 kilobit:** Total bandwidth available to be consumed by this UST-IP unit is limited to the selected quantity. The lower the bandwidth allowed, the slower the performance that may result.
- **Maximum Bandwidth per user:** Sets an upper limit to the amount of bandwidth that can be consumed by each user logged onto this one UST-IP unit.

***Note:** The availability of concurrent remote access is determined by the global setting PC Share Mode on the Security Configuration screen, or individually by user profile through the Keyboard and Mouse Control and Concurrent Access Mode settings on the User Account Settings screen. Control of UST-IP and a connected Target Server is based on first active keyboard/mouse input, so multiple remote users attempting keyboard input or mouse movement at exactly the same moment may experience uneven control.*

- **No Limit (default):** Each active user can consume as much bandwidth as needed.
- **10, 5, 2, or 1 megabit or 512, 256, 128 kilobit:** Bandwidth consumed by each active user during the **operation** of this UST-IP unit is limited to the selected quantity. The lower the bandwidth allowed, the slower the performance that may result.

Press <Ctrl+S> to save changes or <Esc> to cancel changes, and return to Configuration Menu. Saved Performance Settings changes will not take effect until UST-IP is restarted.

Time and Date

Current Date and Time on the UST-IP unit are listed on this screen. Once saved, Time and Date changes will not take effect until UST-IP is restarted.

```

UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.104]

- Time and Date -

Current Date      10/17/2004
Current Time      22:29:35

New Date          [10/17/2004]
New Time          [22:29:35]

Adjust for daylight savings time [NO ]

Get Time From SNTP Server        [NO ]

Time Zone [(GMT-05:00) Eastern Time Zone (US & Canada) ]

CTRL+S - Save Changes  ESC - Cancel Changes  TAB - Next Field

```

- **New Date / New Time:** To manually input changes to current date and time values.
- **Adjust for daylight savings time:** Toggle between YES and NO to reflect whether your country or state follows the daylight savings time procedure.
- **Get Time From SNTP Server:** Indicates whether UST-IP time/date should be automatically synchronized with the time/date of an external SNTP server.
 - **Primary Server IP Address:** IP address of first SNTP server to attempt time synchronization.
 - **Secondary Server IP Address:** IP address of second SNTP server to query, if primary server is unavailable.
 - **User standard UDP port 123:** Allows user to modify UDP port used for SNTP time synchronization. Consult your SNTP server administrator to determine if this value should be adjusted.
- **Time Zone:** Select the time zone in which your UST-IP unit is physically located.

Press <Ctrl+S> to save changes or <Esc> to cancel changes, and return to the Configuration Menu. Saved Radius Configuration changes will not take effect until UST-IP is restarted.

Access Control List

Set UST-IP accessibility in the Access Control List (ACL) to allow or deny specific IP Addresses, or ranges of IP Addresses, from connecting to the UST-IP unit.

If entering a range of IP Addresses, type the starting and the ending IP Address values in the **Start** and **End** columns; use the **TAB** key to navigate through the fields. Use the **←** and **→** keys to select **Allow** or **Deny** for each line item.

```

UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.104]

- Access Control List -
Sl.no.      Start      End      Deny/Allow
-----
1.      [0 . 0 . 0 . 0 ]      [255.255.255.255]      [ALLOW]
2.      [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
3.      [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
4.      [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
5.      [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
6.      [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
7.      [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
8.      [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
9.      [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
10.     [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
11.     [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
12.     [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
13.     [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
14.     [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]
15.     [0 . 0 . 0 . 0 ]      [0 . 0 . 0 . 0 ]      [DENY ]

TAB - Next ACL      CTRL+S - Save Settings
ESC - Exit          N - Next page      P - Previous page

```

Remote Syslog

Use the Remote Syslog Configuration screen to allow remote users to save the server logs. Use the ← and → keys to select **Yes** or **No**.

```
UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.104]
- Remote Syslog Configuration -
Enable Remote Syslog                [NO ]

Press SPACE BAR to toggle the options.

CTRL+S - Save Changes  ESC - Cancel Changes  TAB - Next Field
```

If you select **Yes**, type the IP Address to which you want to save the syslog in the **Remote Syslog Server IP** field, specify the information to save in **Syslog Priority Threshold** (for example, Notices, Debugs, Emergency messages, etc.), and select the category of data in the **Syslog Category** field. Press the **TAB** key to advance through these fields, and use the ← and → keys to make selections.

```
UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.106]
- Remote Syslog Configuration -
Enable Remote Syslog                [YES]

Remote Syslog Server IP              [ 0 . 0 . 0 . 0 ]
Syslog Priority Threshold             [WARNING ]
Syslog Category                      [ALL      ]

Press SPACE BAR to toggle the options.

CTRL+S - Save Changes  ESC - Cancel Changes  TAB - Next Field
```

View UST-IP Status

The UST-IP Event Log screen shows a log file containing information about UST-IP log in and connection activities. This Event Log stores UST-IP events, such as user login or logout, bad login attempts, Admin login, and logout at the UST-IP Admin console, Admin changes to the system configuration, Admin user profile additions, changes, or deletions, modem activity, system startup and shutdown, and all errors that occur, with the date and time of each event. Please see **Appendix D: Troubleshooting** for a listing of error codes with their meaning and suggested solution. Up to 2,048 events can be stored in one log file.

UST-IP also auto-recovers from fatal errors. If a fatal error occurs, it is recorded and UST-IP automatically reboots. If a non-fatal error occurs, it is recorded and UST-IP waits until all users are logged off the system, and then it reboots to make sure the previous non-fatal error does not escalate to a fatal error.

```

UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.104]

- Main Menu -

[C] Configure UST-IP
[V] View UST-IP status
[R] Restart or shutdown the UST-IP
[D] Diagnostics

Press TAB to move to an option and ENTER to select the option.

```

```

UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.104]

Users [1]      Data In [      0]/s      Data Out[ 6767]/s      Activity [kvma]_

Date      Time      Event      [10/17/2004] [22:34:12]
-----
2004-10-17 21:15:17 ADMIN logged in (192.168.51.62)
2004-10-17 21:58:39 ADMIN logged out (192.168.51.62)
2004-10-17 22:18:49 ADMIN logged in (192.168.51.62)
2004-10-17 22:18:54 ADMIN logged out (192.168.51.62)
2004-10-17 22:18:57 ADMIN logged in (192.168.51.62)
2004-10-17 22:19:14 ADMIN logged out (192.168.51.62)
2004-10-17 22:23:02 ADMIN login failed (192.168.50.168)
2004-10-17 22:23:10 ADMIN login failed (192.168.50.168)
2004-10-17 22:23:20 ADMIN logged in (192.168.50.168)
2004-10-17 22:23:44 Anonymous timeout (192.168.51.62)
2004-10-17 22:23:44 Anonymous disconnected (192.168.51.62)
2004-10-17 22:26:51 ADMIN logged in (192.168.51.72)
2004-10-17 22:26:51 ADMIN logged out (192.168.51.72)
2004-10-17 22:32:04 ADMIN logged in (192.168.51.72)
2004-10-17 22:32:04 ADMIN logged out (192.168.51.72)
2004-10-17 22:32:04 ADMIN logged out (192.168.51.72)
<Bottom of the list>

ESC - Exit      N - Next page  P - Previous page  T - Top B - Bottom

```

Restart or Shutdown the UST-IP

Offers options to **Restart** <R>, **Shutdown** <S>, or **Cancel** <Esc> the restart or shutdown command. <R> Restarts the UST-IP unit and brings the UST-IP Admin Console back to the UST-IP Initialization screen.

```

UST-IP v4.10      Name [UST-IP      ]      IP Address [192.168. 51.104]

- Main Menu -

[C] Configure UST-IP
[V] View UST-IP status
[R] Restart or shutdown the UST-IP
[D] Diagnostics

Press TAB to move to an option and ENTER to select the option.

```

Diagnostics

While navigating the Main Menu of the Administrative Console, pressing **<D>** and **<Enter>** will invoke the UST-IP Diagnostic functions.

These functions are meant to enable Raritan Technical Support to assist you in the case of a problem with your UST-IP unit. Do not invoke these functions unless you are fully aware of their meanings and intended use. Please contact Raritan Technical Support should you require more information.

```
-[ UST-IP Diagnostic Console ]-----[ 192.168.051.104 ]-
V      View log                LOG      Set log mask
<ENTER> View more log          M       Insert log marker
P      Pause Log              R       Resume log
C      Clear the log
NETSTATS Network Statistics    PING    Send a network ping
RESET   Reset to factory defaults  RESTART Restarts UST-IP
TRACEROUTE Print the route packetsn and ENTER to select the option.

Type HELP <commandName> to get more information.
Type X   to exit the diagnostic console.
-----
>_
```


Appendix A: Specifications

ITEM	DIMENSIONS (WxDxH)	WEIGHT	POWER
UST-IP1	1U 19" Rackmount Case: 17.2" (W) x 11.46" (D) x 1.72" (H) 440mm (W) x 291mm (D) x 44 mm (H)	8.05 lbs. (3.65 kg)	115V/230V 50/60 Hz 0.3A
UST-IP2	1U 19" Rackmount Case: 17.2" (W) x 11.46" (D) x 1.72" (H) 440mm (W) x 291mm (D) x 44 mm (H)	8.16 lbs. (3.7 kg)	115V/230V 50/60 Hz 0.6A

Remote Connection

Network: 10BASE-T, 100BASE-TX Ethernet
 Modem: Dedicated Modem Port
 Protocols: TCP/IP, UDP, SNMP

Raritan Remote Client (RRC) Software

Operating System Requirements: Windows XP / NT / ME / 2000

KVM Input

Supported Resolutions:

Text Modes	1024x768 @ 60Hz
640x480 @ 60Hz	1024x768 @ 70Hz
640x480 @ 72Hz	1024x768 @ 75Hz
640x480 @ 75Hz	1024x768 @ 85Hz
640x480 @ 85Hz	1152x864 @ 60Hz
800x600 @ 56Hz	1152x864 @ 75Hz
800x600 @ 60Hz	1280x1024 @ 60Hz
800x600 @ 72Hz	
800x600 @ 75Hz	
800x600 @ 85Hz	

Cable Specifications

Category 5e UTP cable to connect to network.

Paragon download cable to connect from Admin Port to local PC port.

KVM Switch Specifications

Supports KVM switches utilizing an On-Screen User Interface, including Raritan's Paragon, Z-Series, MasterConsole MX⁴, and MasterConsole II product lines.

Output Specifications

Local Access Console: PS/2 Keyboard, PS/2 Mouse, HD15 Video
 Local Admin Port: DB9F

Appendix B: SNMP Features

For convenient monitoring with standard network management systems such as HP OpenView or IBM Tivoli software solutions, UST-IP features an SNMP agent with standard MIB2 support. UST-IP responds to SNMP GET requests with standard MIB2 variables, although for security reasons only a subset of the variables are provided.

Appendix C: Frequently Asked Questions

QUESTION:	ANSWER:
What is UST-IP?	UST-IP is the easiest, fastest, most reliable way to remotely access and manage multiple servers connected to a Paragon II - no matter where you are or where your servers are located.
How does UST-IP work?	UST-IP connects to the Cat5 Paragon switch. Using Raritan's powerful frame-grabber and compression technology, it captures, digitizes, and compresses the video signal before transmitting to a remote PC.
What level of control does a UST-IP remote user have over attached Target Servers?	The remote user has direct access and total control of target servers for maintenance, administration, and troubleshooting, from running GUI applications to BIOS-level troubleshooting, and even rebooting.
Remote Access Software has been available for a long time. What makes UST-IP different?	With UST-IP, the UST-IP software runs only on the UST-IP unit itself, not on each individual Target Server. Traditional Remote Access Software solutions require software to be loaded and running on each Target Server, which must offer a supporting Operating System. This can create compatibility, performance, and reliability issues on mission critical Target Servers.
What remote access connection methods can UST-IP accommodate?	UST-IP provides network administrators with a choice of remote access via Internet, LAN/WAN, or dial-up modem. That means servers can be accessed both in and out of band, so remote access to mission-critical target servers is always available - even if the network is down.
What types of computers can UST-IP remotely control?	UST-IP works independently of a Target Server's hardware, operating system, or application software, accessing a Target Server's main input/output devices - keyboard, video, and mouse. Consequently, any hardware that supports standard PC keyboard interfaces, standard PC mouse interfaces, and standard PC video (VGA) can be used with UST-IP.
Is special software required for the Remote PC?	Each UST-IP ships with one copy of UST-IP Control software (TRC). This remote access software runs on any Remote PC with a Windows 98+ operating systems and communicates over Internet, LAN/WAN, or dial-up modem with UST-IP software on the UST-IP unit. With TRC installed, the Remote PC is like any other user console in your KVM configuration, but it can be located anywhere - around the corner, or around the world.
Which Raritan KVM Switches will work with UST-IP?	Currently, UST-IP is supported with the Paragon II line of switches.
Can I continue to access my KVM configuration locally?	Yes. UST-IP features a special Direct Analog User port for direct access to the KVM configuration. This pass through port provides an additional local access point, which is especially important for single user switches or for providing critical access to servers if the network is down.
Does UST-IP support LDAP/RADIUS?	No; it must be part of a Paragon/CommandCenter integration. UST-IP requires the Paragon username and password.
Is UST-IP easy to install?	UST-IP is very easy to install. Just connect it to a user port on an existing KVM configuration and assign an IP address and/or telephone number for modem access.

QUESTION:	ANSWER:
How Is UST-IP administration carried out?	Administrators access UST-IP through a connected UST-IP Admin Console. A simple keyboard driven interface of menus offers straightforward access to UST-IP setup and control. User profiles, security settings, configuration and diagnostics are just a few of the options available. The UST-IP Admin Console can be removed from the server room once initial UST-IP setup is complete, after which all configuration may be performed remotely via web browser.
Are there security features to protect my Target Servers from an unauthorized remote connection?	Yes. UST-IP provides many layers of security. UST-IP can be configured to provide high-level connection authentication and video data transfer security during a remote session. User names, passwords, private-keys, and Secure Socket Layer (SSL) 128-bit encryption are all available. UST-IP can also function as a RADIUS client. In addition, all Raritan KVM Switches that feature an On-Screen User Interface (OSUI) come with a complete security scheme, requiring user name and password access to Servers as designated by the network administrator.
Is there a double login using UST-IP?	No, only single login. A double login exists if you use IP-Reach with Paragon.
Is there Web-Based Access?	Remote access can be obtained via a web browser to the UST-IP1's IP address. <ul style="list-style-type: none"> ▪ Connection from any Windows-based PC - Windows NT, 2000, or XP ▪ Microsoft Internet Explorer 5.5 and 6.0+, Mozilla up to 1.5, and Netscape up to 7.1
How does UST-IP handle a local and remote user when trying to access USTIP?	USTIP1 – the local and remote user share 1 path USTIP2 – the 1st path is shared with local and remote users, the 2 nd path is dedicated for remote users USTIP1 operates under three working modes where the user is able to assign priority to either the local, remote user or provide a “first come first serve basis” via the admin console for the Local port or the Remote port.
Can I customize UST-IP to enhance performance relative to my specific KVM configuration?	Yes. A variety of fine-tuning procedures are available. Automatic Color calibration, KVM On-Screen Display tuning, and Target Mouse Pointer adjustments all serve to enhance UST-IP performance.
Can I customize UST-IP to enhance performance with regard to different remote access methods and situations?	Yes. UST-IP offers a variety of performance enhancements to optimize a chosen connection method. Color Depth, Progressive Update, and Internet Flow Control are just a few of the adjustment options available to speed response time. Color Depth, for example, can be adjusted all the way down to black and white to decrease the data load during an emergency midnight modem connection to mission-critical servers over low-bandwidth.
Can I use UST-IP in a VPN?	Yes. UST-IP fits into most any network configuration utilizing standard TCP/IP. The network administrator simply adds UST-IP as a node on the network via the UST-IP Admin Console.
What is the slowest connection UST-IP can handle?	UST-IP offers scalable performance based on bandwidth available, down to 20kbps.
Can I perform a Dial-up modem connection to UST-IP over a PBX line?	No. Modems require an analog telephone line.
Can I use UST-IP within my local network?	UST-IP can be used in any computer network that supports TCP/IP.

QUESTION:	ANSWER:
When does UST-IP use TCP? UDP?	<p>Both TCP and UDP are used by UST-IP. However, TCP is essential, whereas UDP is optional.</p> <p>UDP is used only for one UST-IP feature, automatic detection (“browse”) of UST-IP units in a subnet (see Chapter 3: Raritan Remote Client, <i>RRC Navigator</i>).</p> <p>If you do not employ the browse feature (and by extension, are not using DHCP), then UST-IP will only communicate using TCP.</p>

Appendix D: Troubleshooting

Problems and Suggested Solutions

REMOTE CONNECTION PROBLEMS	SOLUTION
I cannot connect to UST-IP via dial up modem.	<p>Ensure that you have specified the modem device for your Remote PC in the Add Connection Window (Dial-up type connection) modem field.</p> <p>Although concurrent connections may be enabled (either globally or individually), the modem in UST-IP will only accommodate one remote connection at a time – ensure that someone else is not already connected via modem.</p> <p>Ensure that your user profile has modem access enabled and that UST-IP is configured to enable a modem interface on the Network Configuration Screen.</p> <p>Ensure that the communication port chosen by the network administrator on the Network Configuration screen matches the port set in your connection profile.</p>
I cannot connect to UST-IP via LAN/WAN or Internet.	<p>Re-check the IP settings for UST-IP from the UST-IP Admin Console or remote Admin Console window. Accessing the Network Configuration screen, ensure that the IP addresses set for “IP Address, Subnet Mask, and Default Gateway” are still set correctly, per your Network Administrator’s instructions.</p> <p>Ensure that your user profile has network access enabled and that UST-IP is configured to enable a network interface.</p> <p>Ensure that the communication port chosen by the network administrator on the Network Configuration screen matches the port set in your connection profile.</p> <p>Ensure that the network configuration is correct by sending a PING from the Remote PC to UST-IP.</p>
I cannot connect to UST-IP via Web Browser.	<p>Re-check the IP settings for UST-IP from the UST-IP Admin Console or remote Admin Console window. Accessing the Network Configuration screen, ensure that the IP addresses set for “IP Address, Subnet Mask, and Default Gateway” are still set correctly, per your Network Administrator’s instructions.</p> <p>Ensure that your user profile has Web Browser access enabled and that UST-IP is configured to enable Web Browser.</p>
I cannot connect to UST-IP and seem to be stuck at the Login window.	<p>Ensure that you are using a valid and correct user name and password. Ensure that you are typing user name and password in the exact upper and lowercase combinations in which they were created. Drag the Login window to the side and view Connection Status window behind it. The Connection Status window will show details on your connection attempts, and may offer specifics on the problem.</p>

DIRECT ANALOG USER CONSOLE PROBLEMS	SOLUTION
The Direct Analog User Console does not function.	<p>Make sure the KVM switch is functioning properly. Make sure that UST-IP is turned on. UST-IP must be powered on for the Direct Analog User Console to function. The cable located inside UST-IP that connect the Direct Analog User Console port(s) may have disconnected – Contact Raritan Technical Support for assistance.</p>
I cannot seem to gain steady keyboard/mouse control of the active Target Server	<p>Keyboard/mouse control of a Target Server from a Direct Analog User Console is shared on a first active keyboard/mouse input basis with any remote users who may be currently connected. Ensure that no remote</p>

DIRECT ANALOG USER CONSOLE PROBLEMS	SOLUTION
from a Direct Analog User Console.	users are currently attempting to control the active Target Server.
I cannot view the Target Server that I am looking for from a Direct Analog User Console.	Ensure that you are looking at the Direct Analog User Console connected to the correct User Port. Remember, Direct Analog User Consoles can be attached to User Ports 1 through 4. Each User Console will view the path of the matching KVM Port. For example, the User Console attached to User Port 1 will view the KVM path attached to KVM Port 1. Similarly, the User Console attached to User Port 2 will view the KVM path attached to KVM Port 2, and so on.

KEYBOARD PROBLEMS	SOLUTION
UST-IP is not accepting keyboard commands from the Remote PC.	The UST-IP window of TRC must be the active window for proper keyboard control. Ensure the window in which you are typing is active. Try clearing the keyboard signals to ensure that the release or breakcode signal has been received – alternately press the <Ctrl>, <Shift> and <Tab> keys rapidly a few times on your keyboard. Ensure the remote user has keyboard and mouse privileges. Exit the UST-IP software and then restart it again.
I pressed the Caps Lock key on my Remote PC. The CAPS indicator on the UST-IP Status Bar appeared, but the Caps Lock indicator light is not lit on my Remote PC keyboard.	This is normal. Use the indicators on the Status Bar to determine CAPS key status for the Target Server. If a local user at the Direct Analog User Console's keyboard has changed a Lock key status (Caps-Lock, Num-Lock, or Scroll-Lock) on the Target Server, then server status may not match the state of the Remote PC's keyboard.
The Keyboard is not functioning and the green LED on the back of UST-IP for at least one of the KVM ports is not blinking, but rather constantly lit.	Reset the keyboard chips within UST-IP by recycling power to it. Make sure you power down both UST-IP and all attached KVM switches at the same time. Otherwise the KVM chips in UST-IP will draw power from the KVM switches and fail to reset.
I am accessing UST-IP via the Web Browser and the keyboard does not function. I type, but nothing happens.	Click the window title bar under the UST-IP toolbar to activate the viewing window. If the viewing window is not the active window, the keyboard will not function.

KVM ON-SCREEN USER INTERFACE (OSUI) PROBLEMS	SOLUTION
<p>Clicking on the Enter On-Screen Menu button does not bring up the connected KVM switch's On-Screen User Interface (OSUI). Nothing happens.</p>	<p>UST-IP may not be set to the correct KVM switch Hotkey activator. The default Hotkey setting is <Scroll Lock> or Scroll Lock+Scroll Lock in the UST-IP Options window. Make sure that the Hotkey set in the Options window is the same Hotkey that commands the OSUI of the base KVM switch attached to UST-IP. On the UST-IP window's menu, select Tools > Options. The Options window will appear. Select the appropriate Hotkey, which activates the connected KVM switch's OSUI. Scroll Lock+Scroll Lock = <Scroll Lock>, Num Lock+Num Lock = <Num Lock>, and Caps Lock+Caps Lock = <Caps Lock>. Click [OK] to continue.</p>
<p>A KVM switch is connected to my Remote PC. Entering <ScrollLock> <ScrollLock> (or any other designated KVM switch OSUI Hotkey) from the Remote PC's keyboard activates two OSUIs – one for the KVM switch attached to my Remote PC and one for the base KVM switch attached to UST-IP.</p>	<p>At the Remote PC user console, exit the OSUI for the Remote PC's KVM switch by pressing the <Esc> key once. Wait a few seconds and the OSUI for the Remote PC's KVM switch will disappear. To avoid this problem either reset the Remote PC's attached KVM switch to a Hotkey that differs from the Hotkey for the base KVM switch attached to UST-IP. Or use only UST-IP commands to activate the OSUI for the base KVM switch attached to UST-IP – press the Enter On-Screen Menu button.</p>
<p>Log out of KVM on disconnect is set to YES in the Security Configuration screen, but UST-IP is not logging out of the KVM upon remote user disconnection.</p>	<p>Make sure that the Hotkey set in the Options window is the same Hotkey that commands the OSUI of the base KVM switch attached to UST-IP.</p>

MOUSE PROBLEMS	SOLUTIONS
<p>Target Server Mouse Pointer tracks too slowly after UST-IP Mouse Pointer.</p> <p>Immediately after switching to a new Target Server channel the mouse stops and/or is out of sync.</p>	<p>When working from a Remote PC, a slight delay between the larger UST-IP Mouse Pointer and the smaller Target Server Mouse Pointer is normal due to uncontrollable lags in the speed of the remote connection – Internet, direct dial modem, or network. With each new video image viewed, UST-IP automatically re-syncs and aligns the mouse pointers. Wait a few seconds after switching to each new video image for automatic re-calibration to take place and the two mouse pointers will line up with each other. If you do not wish to wait for this auto calibration, or you find the two mouse pointers out of sync at any time; click Synchronize Mouse, or simultaneously press the keys <Ctrl-Alt-S>. This will manually re-align the two pointers.</p> <p>Adjust the motion of the Target Server Mouse Pointer. For Windows 2000 based Target Servers, set the mouse motion speed on each Target Server to the middle speed setting between slow and fast and the mouse motion acceleration speed on each Target Server to <off> or <none>. For Windows '95, '98, and NT based Target Servers, set the mouse motion speed on each Target Server to the slowest setting.</p> <p>Color Settings are not optimally calibrated. Run the Automatic Color Calibration Routine in Chapter 3: Raritan Remote Client, Color Calibration.</p>

MOUSE PROBLEMS	SOLUTIONS
<p>The larger UST-IP Mouse Pointer does not track or is not in sync (not aligned) with the smaller Target Server Mouse Pointer.</p>	<p>Click Synchronize Mouse, or press <Ctrl-Alt-S>.</p> <p>Ensure each Target Server uses a standard Windows mouse driver.</p> <p>For Windows 2000 based Target Servers, set the mouse motion speed on each Target Server to the middle speed setting between Slow and Fast and the mouse motion acceleration speed on each Target Server to <None>. For Windows '95, '98, and NT based Target Servers, set mouse motion speed on each Target Server to slowest setting possible.</p> <p>Click Auto-sense Video or simultaneously press <Ctrl-Alt-A>.</p>
<p>UST-IP is not accepting my mouse.</p>	<p>UST-IP will not support a serial type mouse or non-standard mouse drivers. It does support a PS/2 style mouse and standard Windows mouse drivers. Other mouse drivers may function with UST-IP, but will require extensive changes to the mouse settings until a functioning mix of motion settings is found. If you must use a mouse driver on a Target Server that is not currently supported by UST-IP, try setting the mouse acceleration to <none> and the mouse speed to <slow>.</p>
<p>UST-IP Mouse Pointer and the Target Server Mouse Pointer do not sync up in certain Windows NT Administration screens, like the NT log on screen.</p>	<p>Windows NT Administration or Log On screens may revert to default mouse pointer motion/acceleration speeds. As a result, mouse sync may not be optimal at these screens. If you are comfortable adjusting the registry on the Windows NT Target Server, you can obtain better UST-IP mouse sync at NT Administration screens by entering the Target Server's registry editor and changing the following settings: default user mouse motion speed = 0; mouse threshold 1 = 0; mouse threshold 2 = 0.</p>

TARGET SERVER PROBLEMS	SOLUTION
<p>When I reboot a Target Server through UST-IP, from a Remote PC, I cannot access the Target Server's BIOS. It seems UST-IP is not accepting the BIOS entry command keystroke.</p>	<p>To access a Target Server's BIOS first temporarily de-select the Sense video mode changes automatically checkbox in the Video Settings window, accessed with Video Settings on the UST-IP toolbar. Video auto-sensing slows remote viewing of the reboot process and makes it difficult to send BIOS access keystrokes to the Target Server from a Remote PC, because auto-sensing tells UST-IP to work constantly to keep up with the Target Server's feverishly changing video screens during reboot. De-selecting the auto-sense checkbox frees UST-IP to accept and convey BIOS access keystrokes. It also aides in the quick interpretation of rapidly changing video screens. Be sure to re-select the checkbox when finished with BIOS access.</p>

UST-IP PROBLEMS	SOLUTION
There is no control and no frame grabbing activity occurring. UST-IP seems to have locked-up.	An internal serial data cable, which connects the frame grabber card to the motherboard of UST-IP, may have become disconnected. Contact Raritan Technical Support for assistance.
I cannot power down UST-IP.	The main power switch for UST-IP is on the back of the unit. To turn off UST-IP hold the power key down for a few seconds. To turn UST-IP back on, press the power button again.
After loss of power UST-IP does not automatically power-ON again when power is regained.	Enter the BIOS of UST-IP and ensure that the “Power Lost Resume State” is set to “Last State.” UST-IP will then turn ON when power is applied only if it was already ON when power was lost.

VIDEO PROBLEMS	SOLUTION
After switching to a different Target Server channel the video is not clear. Sometimes there is a black edge at the boundary of the Target Server’s screen.	Click Auto-sense Video or simultaneously press the keys <Ctrl-Alt-A>. UST-IP will adjust the video settings. If the video does not become clear, additional manual video setting adjustments may be necessary. Contact Raritan Technical Support to discuss changes to the Video Settings window. Ensure all Target Servers have standard blanking times. Horizontal and vertical blanking times should closely approximate VESA standard values.
When viewing a Target Server remotely, the video image is filled with moving block of incorrect color that seem to track next to the movement of the mouse pointer.	The Color Settings on the Video Settings tab in the Video window are not set correctly. Attempt manual adjustment until the color blocking ceases or run the Automatic Color Calibration Routine (see Chapter 3: Raritan Remote Client, Color Calibration).
The screen is filled with small visual errors, or grains of missing color, which need to be cleaned up.	Click Refresh Screen on the UST-IP toolbar or simultaneously press the keys <Ctrl-Alt-R>.
The video seems to be stuck in Auto Sense mode and the auto sensing message in the middle of the screen keeps counting higher and higher.	Pressing Auto-sense Video while auto sensing is occurring will stop the auto sense process. Check your Target Server resolution to ensure UST-IP supports it.

WEB BROWSER PROBLEMS	SOLUTION
I cannot connect to UST-IP via Web Browser.	Re-check the IP settings for UST-IP from the UST-IP Admin Console or remote Admin Console window. Accessing the Network Configuration screen, ensure that the IP addresses set for “IP Address, Subnet Mask, and Default Gateway” are still set correctly, per your Network Administrator’s instructions. Ensure that your user profile has Web Browser access enabled and that UST-IP is configured to enable Web Browser.

Event Log File and On-Screen Error Codes

UST-IP will display or log an error code in the **UST-IP Event Log Screen** in the event of a problem occurring. Error codes are eight-digit hexadecimal numbers, containing two parts: the first four denote error type; and the second four digits denote a location code.

These last four digits of the UST-IP error code are the most useful in determining what has caused a system failure. Below is a list of location codes (the last four digits of an error code), and their meanings.

ERROR CODE (LAST 4 DIGITS)	MEANING	RECOMMENDATION
0001 – 0003	Memory allocation error	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0004	Could not read the configuration file on startup. The file may be corrupt, the file system may be damaged, or the config file might be from an older version of UST-IP.	Reenter the configuration information and reboot. If the problem continues, restore the software and file system from the Recovery CD-ROM.
0005	The config file was missing. This may be the first time you have started UST-IP or the file system has become corrupt.	Reenter the configuration information and reboot. If the problem continues, restore the software and file system from the Recovery CD-ROM.
0006	The config file could not be saved. The file system may be corrupt or the hard drive may not be responding.	Retry, but if the problem persists, restore the software and file system from the Recovery CD-ROM.
0007 – 0008	Memory allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
Delete	Memory allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the recovery CD-ROM.
0009	Could not find the frame grabber card.	Power off the system and make sure the frame grabber card is inserted firmly. If the problem persists, there may be a problem with your UST-IP hardware.
000A	Frame grabber card is not responding correctly.	Power off the system and make sure the frame grabber card is inserted firmly. If the problem persists, there may be a problem with your UST-IP hardware.
000B	Memory allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
000C – 000F	Memory allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.

ERROR CODE (LAST 4 DIGITS)	MEANING	RECOMMENDATION
0011	The Ethernet controller could not be found.	There is a problem with the UST-IP hardware.
0012	The modem could not be found.	Power off the system and make sure the frame grabber card is inserted firmly. If the problem persists, there may be a problem with your UST-IP hardware.
0013	Memory allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0014	There is a problem with the IP address.	Check the IP address configuration and reboot.
0015	The DHCP server did not respond. UST-IP could not acquire an IP address.	Make sure your DHCP server is operating correctly and then reboot UST-IP.
0016 – 0019	There is a problem with one of the UST-IP startup files.	Restore the software and file system from the Recovery CD-ROM.
001A	Error occurred while initializing the UDP socket.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001B	Error occurred while initializing the TCP write socket.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001C	Error occurred while initializing the TCP read socket.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001D – 001E	Resource allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
001F	Could not listen to the TCP write socket.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0020	Could not listen to the TCP read socket.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0021	TCP listen process failed.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0022	UDP listen process failed.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0023	SSL write failed.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the

ERROR CODE (LAST 4 DIGITS)	MEANING	RECOMMENDATION
		Recovery CD-ROM.
0024	SSL read failed.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0025	Memory allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0026 – 0029	Resource allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
002A – 002F	Resource allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0030-0039	Resource allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
003A – 003F	Resource allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.
0040	Resource allocation error.	Reboot UST-IP. Make sure the BIOS memory test recognizes at least 64MB of RAM. If the problem persists, restore the software and file system from the Recovery CD-ROM.